LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz
802.11g

Wireless-G

ADSL Gateway

User Guide

WIRELESS

Model No. **WAG54G**

CISCO SYSTEMS

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

How to Use this Guide

Your Guide to the Wireless-G ADSL Gateway has been designed to make understanding networking with the Gateway easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a Note of interest and is something you should pay special attention to while using the Gateway.

This exclamation point means there is a Caution or Warning and is something that could damage your property or the Gateway.

This question mark provides you with a reminder about something you might need to do while using the Gateway.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

Chapter 1: Introduction 1
- Welcome 1
- What's in this Guide? 2

Chapter 2: Planning Your Network 4
- The Gateway's Functions 4
- IP Addresses 4
- Why do I need a VPN? 5
- What is a VPN? 6

Chapter 3: Getting to Know the Wireless-G ADSL Gateway 8
- The Back Panel 8
- The Front Panel 9

Chapter 4: Connecting the Wireless-G Broadband Gateway 10
- Overview 10
- Wired Connection to a Computer 11
- Wireless Connection to a Computer 11

Chapter 5: Configuring the Gateway 13
- Overview 13
- How to Access the Web-based Utility 15
- The Setup Tab 15
- The Wireless Tab 23
- The Security Tab 26
- The Access Restrictions Tab 31
- The Applications and Gaming Tab 33
- The Administration Tab 36
- The Status Tab 41

Appendix A: Troubleshooting 45
- Common Problems and Solutions 45
- Frequently Asked Questions 53

Appendix B: Wireless Security 59

Appendix C: Configuring IPSec between a Windows 2000 or XP Computer and the Gateway 62
- Introduction 62

Environment 62
How to Establish a Secure IPSec Tunnel 63
Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter 73
Windows 98 or Me Instructions 73
Windows 2000 or XP Instructions 74
Appendix E: Upgrading Firmware 75
Appendix F: Glossary 76
Appendix G: Specifications 82
Appendix H: Regulatory Information 84
Appendix I: Warranty Information 87
Appendix J: Contact Information 88

List of Figures

Figure 2-1: Network 4
Figure 2-2: VPN Gateway-to-VPN Gateway 7
Figure 2-3: Computer-to-VPN Gateway 8
Figure 3-1: Back Panel 9
Figure 3-2: Front Panel 10
Figure 4-1: LAN Connection 12
Figure 4-2: ADSL Connection 12
Figure 4-3: Power Connection 12
Figure 5-1: Password Screen 16
Figure 5-2: Basic Setup Tab 16
Figure 5-3: Dynamic IP 17
Figure 5-4: Static IP 17
Figure 5-5: RFC 1483 Routed 18
Figure 5-6: RFC 2516 PPPoE 18
Figure 5-7: RFC 2364 PPoA 19
Figure 5-8: Bridged Mode Only 19
Figure 5-9: Optional Settings 20
Figure 5-10: DynDNS.org 21
Figure 5-11: Advanced Routing 22
Figure 5-12: Routing Table 23
Figure 5-13: 64-Bit WEP Encryption 24
Figure 5-14: 128-Bit WEP Encryption 24
Figure 5-15: Wireless Network Access 25
Figure 5-16: Networked Computers 25
Figure 5-17: Advanced Wireless Settings 26
Figure 5-18: Firewall 27
Figure 5-19: VPN 28
Figure 5-20: Manual Key Management 29
Figure 5-21: Advanced VPN Tunnel Setup 30
Figure 5-22: Access Restriction 32

Figure 5-23: Internet Policy Summary 32
Figure 5-24: List of PCs 33
Figure 5-25: Port Services 33
Figure 5-26: Single Port Forwarding 34
Figure 5-27: Port Range Forwarding 35
Figure 5-28: Port Triggering 35
Figure 5-29: DMZ 36
Figure 5-30: Management 37
Figure 5-31: Reporting 39
Figure 5-32: Ping Test 40
Figure 5-33: Factory Defaults 40
Figure 5-34: Firmware Upgrade 41
Figure 5-35: Status 42
Figure 5-36: Local Network 43
Figure 5-37: DHCP Clients Table 43
Figure 5-38: Wireless 44
Figure 5-39: DSL Connection 45
Figure C-1: Password Screen 64
Figure C-2: Setup Tab 64
Figure C-3: IP Filter List Tab 64
Figure C-4: IP Filter List 65
Figure C-5: Filters Properties 65
Figure C-6: New Rule Properties 65
Figure C-7: IP Filter List 66
Figure C-8: Filters Properties 66
Figure C-9: New Rule Properties 66
Figure C-10: IP Filter List Tab 67
Figure C-11: Filter Action Tab 67
Figure C-12: Security Methods Tab 67
Figure C-13: Authentication Methods 68
Figure C-14: Preshared Key 68
Figure C-15: New Preshared Key 68
Figure C-16: Tunnel Setting Tab 69

Figure C-17: Connection Type Tab 69
Figure C-18: Properties Screen 69
Figure C-19: IP Filter List Tab 70
Figure C-20: Filter Action Tab 70
Figure C-21: Authentication Methods Tab 70
Figure C-22: Preshared Key 71
Figure C-23: New Preshared Key 71
Figure C-24: Tunnel Setting Tab 71
Figure C-25: Connection Type 72
Figure C-26: Rules 72
Figure C-27: Local Computer 72
Figure D-1: IP Configuration Screen 74
Figure D-2: MAC Address/Adapter Address 74
Figure D-3: MAC Address/Physical Address 75
Figure E-1: Upgrade Firmware 77

Chapter 1: Introduction

Welcome

The Linksys Wireless-G ADSL Gateway is the all-in-one solution for Internet connectivity in your home. The ADSL Modem function gives you a blazing fast connection to the Internet, far faster than a dial-up, and without tying up your phone line.

Connect your computers to the Gateway via the built-in 4-port 10/100 Ethernet Switch to jump start your home network. You can share files, printers, hard drive space and other resources, or play head-to-head computer games. Attach four computers directly, or connect more hubs and switches to create as big a network as you need. The built-in Wireless-G (802.11g) Access Point allows up to 32 wireless devices to connect to your network at a blazing 54Mbps, without running cables through the house. It's also compatible with Wireless-B (802.11b) devices, at 11Mbps. The Gateway ties it all together and lets your whole network share that high-speed Internet connection.

To protect your data and privacy, the Wireless-G ADSL Gateway features an advanced firewall to keep Internet intruders and attackers out. Wireless transmissions can be protected by powerful data encryption. Safeguard your family with Parental Control features like Internet Access Time Limits and Key Word Blocking. Configuration is a snap with any web browser.

With the Linksys Wireless-G ADSL Gateway at the heart of your home network, you're connected to the future.

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G ADSL Gateway.

- Chapter 1: Introduction
  This chapter describes the Wireless-G ADSL Gateway Wireless-G ADSL Gateway applications and this User Guide.

- Chapter 2: Planning Your Network
  This chapter describes the basics of networking.

- Chapter 3: Getting to Know the Wireless-G ADSL Gateway
  This chapter describes the physical features of the Gateway.

- Chapter 4: Connecting the Wireless-G ADSL Gateway
  This chapter instructs you on how to connect the Gateway to your network.

- Chapter 5: Configuring the Gateway
  This chapter explains how to use the Web-Based Utility to configure the settings on the Gateway.

- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-G ADSL Gateway.

- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.

- Appendix C: Configuring IPSec between a Windows 2000 Computer and the Gateway
  This appendix instructs you on how to establish a secure IPSec tunnel using preshared keys to join a private network inside the VPN Gateway and a Windows 2000 or XP computer.

- Appendix D: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on your Gateway if you should need to do so.

- Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter.
  This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Gateway.

- Appendix F: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

- Appendix G: Specifications
  This appendix provides the technical specifications for the Gateway.

- Appendix H: Warranty Information
  This appendix supplies the warranty information for the Gateway.

- Appendix I: Regulatory Information
  This appendix supplies the regulatory information regarding the Gateway.

- Appendix J: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Network

The Gateway's Functions

A Gateway is a network device that connects two networks together.

In this instance, the Gateway connects your Local Area Network (LAN), or the group of computers in your home or office, to the Internet. The Gateway processes and regulates the data that travels between these two networks.

The Gateway's NAT feature protects your network of computers so users on the public, Internet side cannot "see" your computers. This is how your network remains private. The Gateway protects your network by inspecting every packet coming in through the Internet port before delivery to the appropriate computer on your network. The Gateway inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate computer on the LAN side.

Remember that the Gateway's ports connect to two sides. The LAN ports connect to the LAN, and the ADSL port connects to the Internet. The LAN ports transmit data at 10/100Mbps.

Figure 2-1: Network

***LAN**: the computers and networking products that make up your local network*

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including computers, print servers, and Gateways, requires an IP address to identify its "location," or address, on the network. This applies to both the Internet and LAN connections. There are two ways of assigning an IP address to your network devices. You can assign static IP addresses or use the Gateway to assign IP addresses dynamically.

Static IP Addresses

A static IP address is a fixed IP address that you assign manually to a computer or other device on the network. Since a static IP address remains valid until you disable it, static IP addressing ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses must be unique and are commonly used with network devices such as server computers or print servers.

NOTE: Since the Gateway is a device that connects two networks, it needs two IP addresses—one for the LAN, and one for the Internet. In this User Guide, you'll see references to the "Internet IP address" and the "LAN IP address."

Since the Gateway uses NAT technology, the only IP address that can be seen from the Internet for your network is the Gateway's Internet IP address. However, even this Internet IP address can be blocked, so that the Gateway and network seem invisible to the Internet—see the Block WAN Requests description under Security in "Chapter 5: Configuring the Gateway."

Since you use the Gateway to share your DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Gateway. You can get that information from your ISP.

Dynamic IP Addresses

A dynamic IP address is automatically assigned to a device on the network, such as computers and print servers. These IP addresses are called "dynamic" because they are only temporarily assigned to the computer or device. After a certain time period, they expire and may change. If a computer logs onto the network (or the Internet) and its dynamic IP address has expired, the DHCP server will automatically assign it a new dynamic IP address.

DHCP (Dynamic Host Configuration Protocol) Servers

Computers and other network devices using dynamic IP addressing are assigned a new IP address by a DHCP server. The computer or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated computer on the network or another network device, such as the Gateway. By default, the Gateway's DHCP Server function is enabled.

If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Gateway, see the DHCP section in "Chapter 5: Configuring the Gateway."

What is a VPN?

A VPN, or Virtual Private Network, is a connection between two endpoints - a VPN Gateway, for instance - in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a "tunnel". A VPN tunnel connects the two computers or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices,

telecommuters, and/or professionals on the road (travelers can connect to a VPN Gateway using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

- VPN Gateway to VPN Gateway
- Computer (using VPN client software that supports IPSec) to VPN Gateway

The VPN Gateway creates a "tunnel" or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software that supports IPSec can be one of the two endpoints. Any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the VPN Gateway to create a VPN tunnel using IPSec (refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway"). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

Computer (using VPN client software that supports IPSec) to VPN Gateway

The following is an example of a computer-to-VPN Gateway VPN. (See Figure 2-2.) In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the VPN Gateway at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

Figure 2-2: Computer-to-VPN Gateway

VPN Gateway to VPN Gateway

An example of a VPN Gateway-to-VPN Gateway VPN would be as follows. (See Figure 2-3.) At home, a telecommuter uses his VPN Gateway for his always-on Internet connection. His Gateway is configured with his office's VPN settings. When he connects to his office's Gateway, the two Gateways create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

For additional information and instructions about creating your own VPN, please visit Linksys's international website at www.linksys.com/international or refer to "Appendix C: Configuring IPSec between a Windows 2000 or XP computer and the VPN Gateway."

IMPORTANT: You must have at least one VPN Gateway on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second VPN Gateway or a computer with VPN client software that supports IPSec.

Why do I need a VPN?

Computer networking provides a flexibility not available when using a paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to

protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network - when you send data to someone via email or communicate with an individual over the Internet - the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Data “sniffing” is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the Middle Attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a “man in the middle” attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

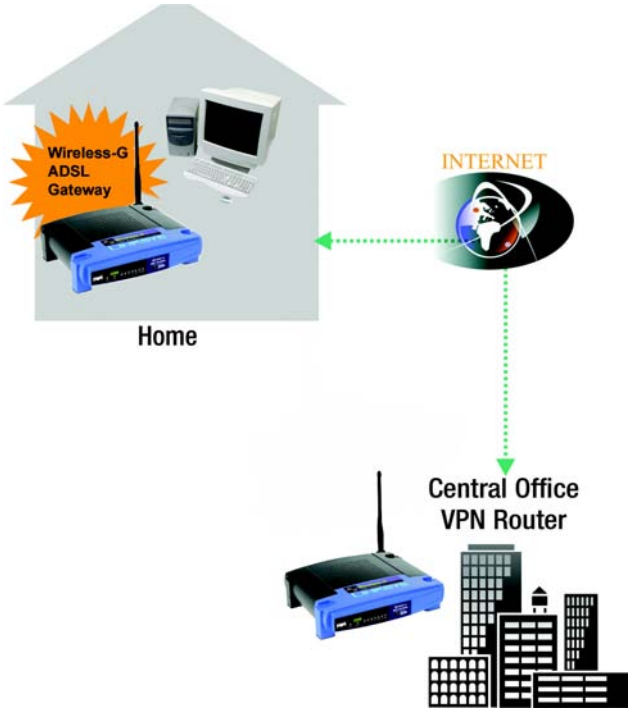

Figure 2-3: VPN Gateway-to-VPN Gateway

Chapter 3: Getting to Know the Wireless-G ADSL Gateway

The Back Panel

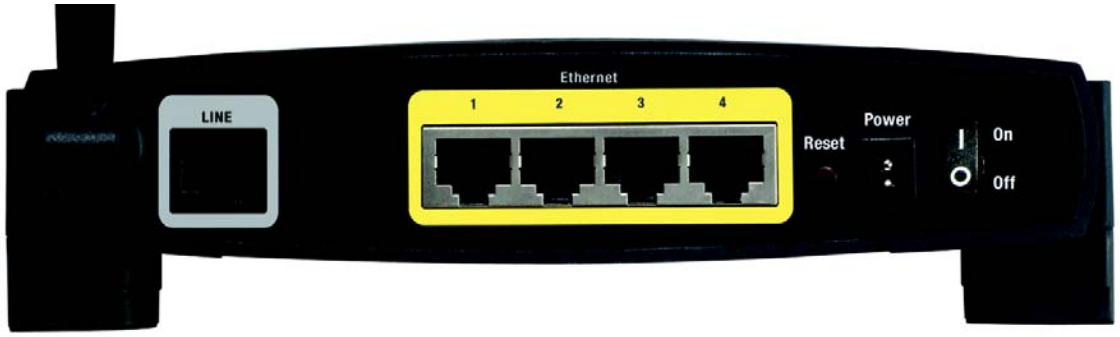

Figure 3-1: Back Panel

The Gateway's ports, where a network cable is connected, are located on the back panel. The Gateway's buttons are also located on the back panel.

LINE The **LINE** port connects to the ADSL line.

Ethernet (1-4) The **Ethernet** ports connect to your computer and other network devices.

Power The **Power** port is where you will connect the power adapter.

Reset Button There are two ways to Reset the Gateway's factory defaults. Either press the **Reset Button**, for approximately ten seconds, or restore the defaults from the Factory Defaults screen of the Administration tab in the Gateway's Web-Based Utility.

On/Off This switch is used to turn the Gateway on or off.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys international website at www.linksys.com/international for more information about products that work with the Gateway.

Important: Resetting the Gateway to factory defaults will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Gateway if you want to retain these settings.

The Front Panel

The Gateway's LEDs, where information about network activity is displayed, are located on the front panel.

Figure 3-2: Front Panel

Power Green. The **Power** LED lights up when the Gateway is powered on.

Ethernet (1-4) Green. The **LAN** LED serves two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through the LAN port. If the LED is blinking, it is an indication of any network activity.

WLAN Green. The **WLAN** LED lights up whenever there is a successful wireless connection. If the LED is blinking, the Gateway is actively sending or receiving data to or from one of the devices on the network.

DSL Green. The **DSL** LED lights up whenever there is a successful DSL connection. The LED blinks while establishing the ADSL connection.

Internet Green. The **Internet** LED lights up green when an Internet connection to the Internet Service Provider (ISP) session is established. The **Internet** LED lights up red when the connection to the ISP fails.

Chapter 4: Connecting the Wireless-G Broadband Gateway

Overview

The Gateway's setup consists of more than simply plugging hardware together. You will have to configure your networked computers to accept the IP addresses that the Gateway assigns them (if applicable), and you will also have to configure the Gateway with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information for your modem with you after installing your broadband connection. If not, you can call your ISP to request that data.

After you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Gateway.

If you want to use a computer with an Ethernet adapter to configure the Gateway, continue to "Wired Connection to a computer." If you want to use a computer with a wireless adapter to configure the Gateway, continue to "Wireless Connection to a Computer."

Wired Connection to a Computer

1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.
2. Connect one end of an Ethernet network cable to one of the Ethernet ports (labeled 1-4) on the back of the Gateway (see Figure 4-1), and the other end to an Ethernet port on a computer.
3. Repeat this step to connect more computers, a switch, or other network devices to the Gateway.

IMPORTANT: If using microfilters, make sure to only place the microfilters between the phone and the wall jack and not between the Gateway and the wall jack or your ADSL will not connect.

4. Connect a phone cable from the Line port on the Gateway's back panel (see Figure 4-2) to the wall jack of the ADSL line. A small device called a microfilter may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.
5. Connect the power adapter to the Gateway's Power port (see Figure 4-3), and then plug the power adapter into a power outlet. Turn the On/Off switch to On.
   - The Power LED on the front panel will light up green as soon as the power adapter is connected properly and the switch is turned on. The Power LED will flash for a few seconds, then it will light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."
6. Power on one of your computers that is connected to the Gateway.

Figure 4-1: Ethernet Connection

Figure 4-2: ADSL Connection

NOTE: You should always plug the Gateway's power adapter into a power strip with surge protection.

Wireless Connection to a Computer

If you want to use a wireless connection to access the Gateway, follow these instructions:

1. Before you begin, make sure that all of your network's hardware is powered off, including the Gateway and all computers.

Figure 4-3: Power Connection

IMPORTANT: If using microfilters, make sure to only place the microfilters between the phone and the wall jack and not between the Gateway and the wall jack or your ADSL will not connect.

2. Connect a phone cable from the Line port on the Gateway's back panel (see Figure 4-2) to the wall jack of the ADSL line. A small device called a microfilter may be necessary between each phone and wall jack to prevent interference. Contact your ISP if you have any questions.

3. Connect the power adapter to the Power port (see Figure 4-3), and then plug the power adapter into a power outlet. Turn the On/Off switch to On.

   - The Power LED on the front panel will light up green as soon as the power adapter is connected properly and the switch is turned on. The Power LED will flash for a few seconds, then light up steady when the self-test is complete. If the LED flashes for one minute or longer, see "Appendix A: Troubleshooting."

4. Power on one of the computers on your wireless network(s).

5. For initial access to the Gateway through a wireless connection, make sure the computer's wireless adapter has its SSID set to linksys (the Gateway's default setting), and its WEP encryption is disabled. After you have accessed the Gateway, you can change the Gateway and this computer's adapter settings to match the your usual network settings.

NOTE: You should always change the SSID from its default, linksys, and enable WEP encryption.

The Gateway's hardware installation is now complete.

Go to "Chapter 5: Configuring the Gateway."

Chapter 5: Configuring the Gateway

Overview

Follow the steps in this chapter and use the Gateway's web-based utility to configure the Gateway. This chapter will describe each web page in the Utility and each page's key functions. The utility can be accessed via your web browser through use of a computer connected to the Gateway. For a basic network setup, most users only have to use the following screens of the Utility:

- Basic Setup. On the Basic Setup screen, enter the settings provided by your ISP.
- Management. Click the **Administration** tab and then the **Management** tab. The Gateway's default username and password is admin. To secure the Gateway, change the Password from its default.

There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

Have You: Enabled TCP/IP on your computers? computers communicate over the network with this protocol. Refer to Appendix D: Windows Help for more information on TCP/IP.

Note: For added security, you should change the password through the Administration tab.

Setup

- Basic Setup. Enter the Internet connection and network settings on this screen.
- DDNS. To enable the Gateway's Dynamic Domain Name System (DDNS) feature, complete the fields on this screen.
- Advanced Routing. On this screen, you can alter Dynamic Routing, and Static Routing configurations.

Wireless

- Basic Wireless Settings. You can choose your Wireless Network Mode and Wireless Security on this screen.
- Wireless Network Access. This screen displays your wireless network access list.
- Advanced Wireless Settings. On this screen you can access the Advanced Wireless features.

Security

- Firewall. This screen contains Filters and Block WAN Requests. Filters block specific internal users from accessing the Internet and block anonymous Internet requests.

- VPN. To enable or disable IPSec and/or PPTP Pass-through, and set up VPN tunnels, use this screen.

Access Restrictions

- Internet Access. This screen allows you to prevent or permit only certain users from attaching to your network.

Applications & Gaming

- Single Port Forwarding. Use this screen to set up common services or applications on your network.
- Port Range Forwarding. To set up public services or other specialized Internet applications on your network, click this tab.
- Port Triggering. To set up triggered ranges and forwarded ranges for Internet applications, click this tab.
- DMZ. To allow one local user to be exposed to the Internet for use of special-purpose services, use this screen.

Administration

- Management. On this screen, alter Gateway access privileges, SNMP, and UPnP settings.
- Reporting. If you want to view or save activity logs, click this tab.
- Diagnostics. Use this screen to do a Ping Test.
- Factory Defaults. If you want to restore the Gateway's factory defaults, use this screen.
- Firmware Upgrade. Click this tab if you want to upgrade the Gateway's firmware.

Status

- Gateway. This screen provides status information about the Gateway.
- Local Network. This provides status information about the local network.
- Wireless. This screen provides status information about the wireless network.
- DSL Connection. This screen provides status information about the DSL connection.

How to Access the Web-based Utility

To access the web-based utility, launch Internet Explorer or Netscape Navigator, and enter the Gateway's default IP address, 192.168.1.1, in the Address field. Then press Enter.

A password request page, shown in Figure 5-1 will appear. (non-Windows XP users will see a similar screen.) Enter **admin** (the default user name) in the User Name field, and enter **admin** (the default password) in the Password field. Then click the **OK** button.

Some of the screens and their features may differ from the descriptions in this User Guide, depending on which version of the firmware the Gateway is using.

Figure 5-1: Password Screen

The Setup Tab

The Basic Setup Tab

The first screen that appears is the Basic Setup tab. (See Figure 5-2.) This tab allows you to change the Gateway's general settings. Change these settings as described here and click the **Save Settings** button to save your changes or **Cancel Changes** to cancel your changes.

Internet Setup

- VC Settings. Virtual Circuits (VPI and VCI): These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Your ISP will provide the correct settings for these fields. Multiplexing: Select **LLC** or **VC**, depending on your ISP.
- ADSL Settings. The Gateway supports five Encapsulations: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA, and Bridged Mode Only. Each Basic Setup screen and available features will differ depending on what type of encapsulation you select.

RFC 1483 Bridged

Dynamic IP

IP Settings. Select **Obtain an IP Address Automatically** if your ISP says you are connecting through a dynamic IP address. (See Figure 5-3.)

Figure 5-2: Basic Setup Tab

Static IP

If you are required to use a permanent IP address to connect to the Internet, then select **Use the following IP Address**. (See Figure 5-4.)

- IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

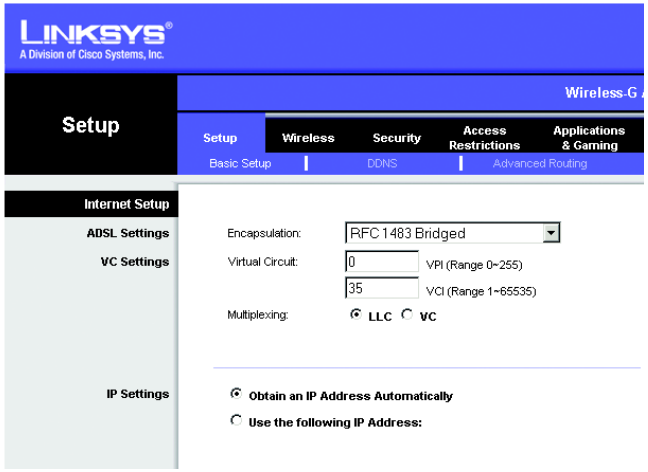

Figure 5-3: Dynamic IP

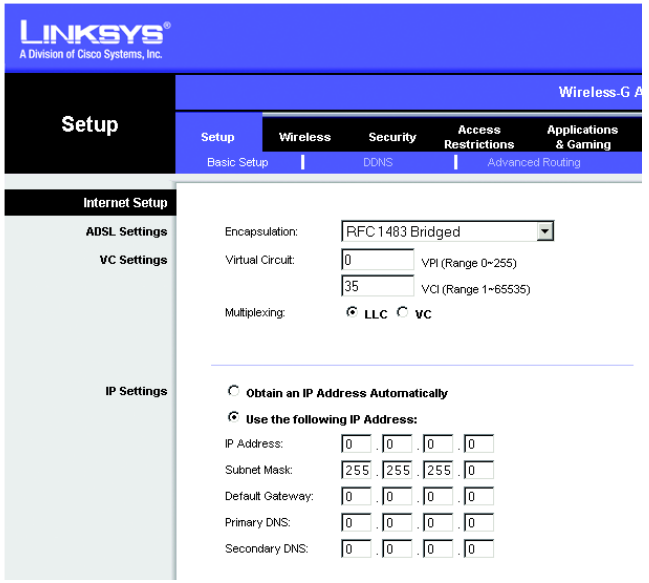

Figure 5-4: Static IP

RFC 1483 Routed

If you are required to use RFC 1483 Routed, then select **RFC 1483 Routed**. (See Figure 5-5.)

- IP Address. This is the Gateway's IP address, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.
- Subnet Mask. This is the Gateway's Subnet Mask. Your ISP will provide you with the Subnet Mask.
- Default Gateway. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.
- Primary DNS. (Required) and Secondary DNS (Optional). Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

RFC 2516 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. (See Figure 5-6.)

- Service Name. Enter the Service Name, if required by your ISP.
- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to disconnect the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is 30 seconds.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

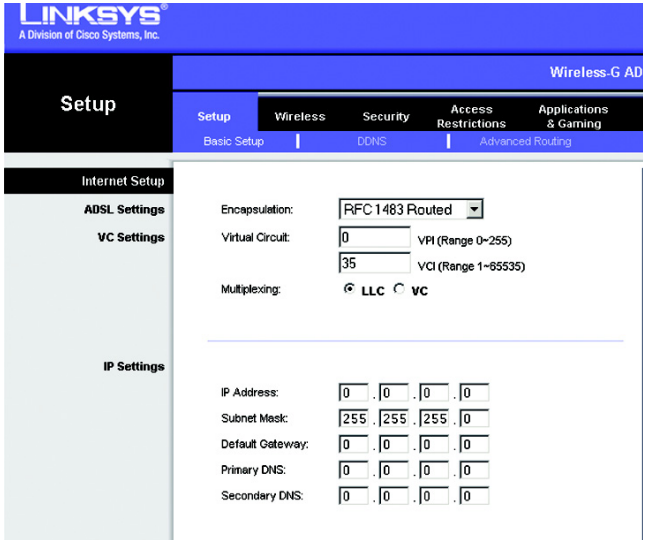

Figure 5-5: RFC 1483 Routed

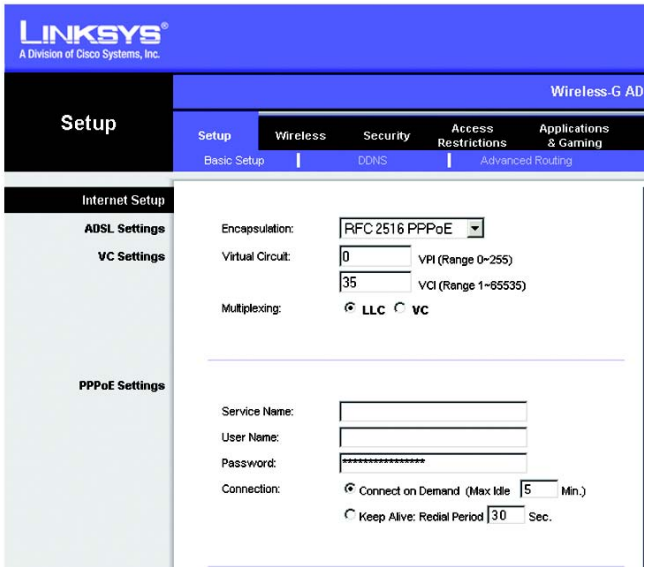

Figure 5-6: RFC 2516 PPPoE

RFC 2364 PPPoA

Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA. (See Figure 5-7.)

- User Name and Password. Enter the User Name and Password provided by your ISP.
- Connect on Demand: Max Idle Time. You can configure the Gateway to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- Keep Alive Option: Redial Period. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. In the Redial Period field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is 30 seconds.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

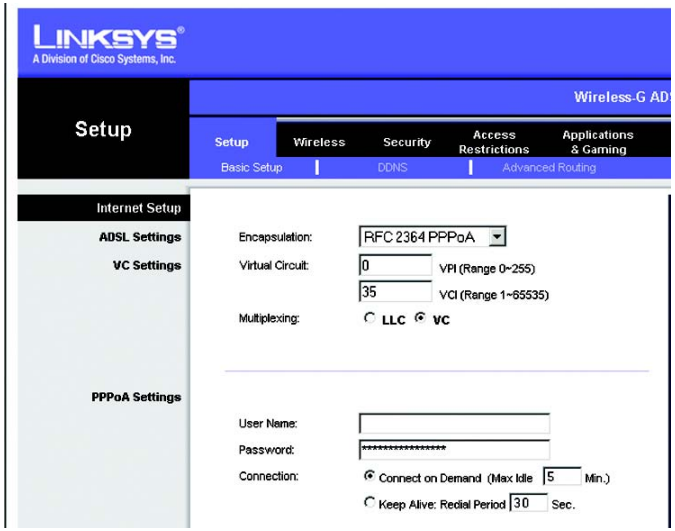

Figure 5-7: RFC 2364 PPPoA

Bridged Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a standalone modem, select **Bridged Mode Only**. (see Figure 5-8). All NAT and routing is disabled in this mode.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

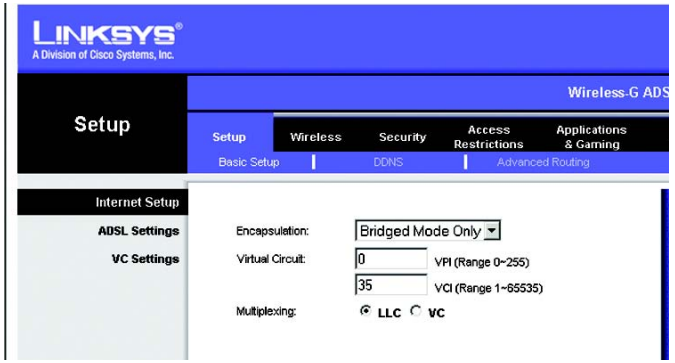

Figure 5-8: Bridged Mode Only

Optional Settings (Required by some ISPs) (See Figure 5-9.)

- Host Name and Domain Name. These fields allow you to supply a host and domain name for the Gateway. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

- MTU. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. Select **Manual** and enter the value desired. It is recommended that you leave this value in the 1200 to 1500 range. By default, MTU is configured automatically.

Network Setup

- Router IP. The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.
  - Local IP Address. The default value is 192.168.1.1.
  - Subnet Mask. The default value is 255.255.255.0.
- Network Address Server Settings (DHCP). A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, it is highly recommended that you leave the Gateway enabled as a DHCP server.
  - Local DHCP Server. DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Gateway's DHCP option to **Disable**.
  - Starting IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1. 2 or greater, because the default IP address for the Gateway is 192.168.1.1.
  - Number of Address. Enter the maximum number of computers that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. By default, as shown in Figure 5-9, the range is 192.168.1.100 to 192.168.1.149.
  - DHCP Address Range. The range of DHCP addresses is displayed here.
  - Client Lease Time. Enter the minutes in the field.
- Time Setting. This is where you set the time zone for your Gateway.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

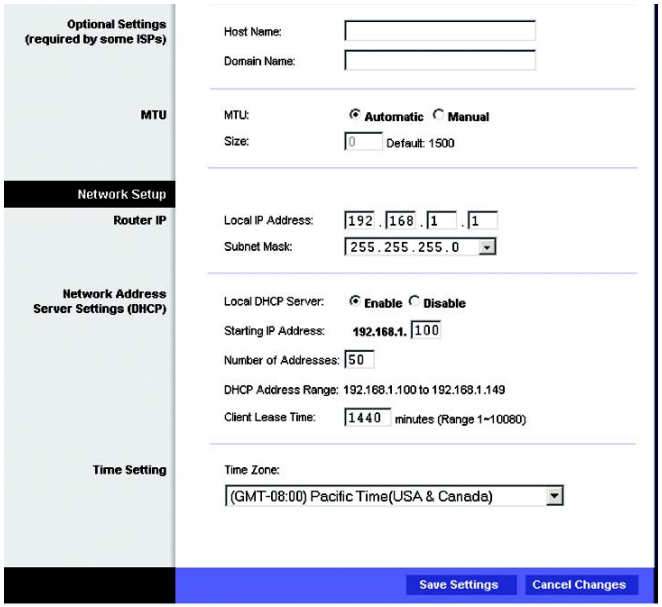

Figure 5-9: Optional Settings

The DDNS Tab

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service at DynDNS.org.

DDNS

DDNS Service. If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** in the drop-down menu. (See Figure 5-10.) To disable DDNS Service, select **Disabled**.

DynDNS.org

- User Name, Password, and Host Name. Enter the User Name, Password, and Host Name of the account you set up with DynDNS.org.
- Internet IP Address. The Gateway's current Internet IP Address is displayed here. Because it is dynamic, it will change.
- Status. The status of the DDNS service connection is displayed here.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-10: DynDNS.org

Advanced Routing Tab

The Advanced Routing screen allows you to configure the dynamic routing and static routing settings. (See Figure 5-11.)

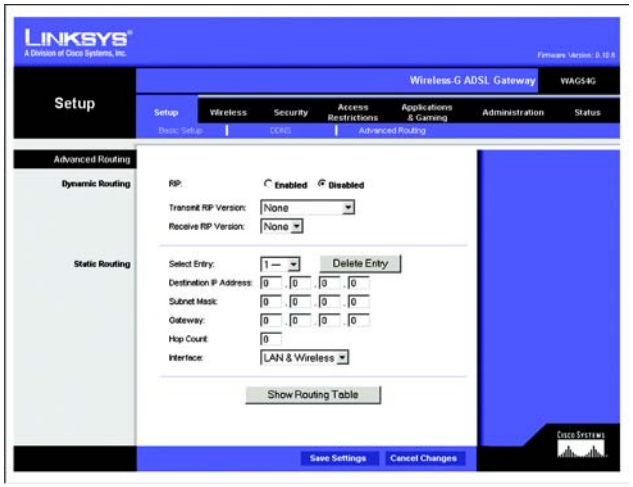

Figure 5-11: Advanced Routing

Advanced Routing

- Dynamic Routing. With Dynamic Routing you can enable the Gateway to automatically adjust to physical changes in the network's layout. The Gateway, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other Gateways on the network. To enable RIP, click **Enabled**. To disable RIP, click **Disabled**.
- Receive RIP Version. To receive RIP messages, select the protocol you want: **RIP1** or **RIP2**. If you don't want to receive RIP messages, select **None**.
- Transmit RIP Version. To transmit RIP messages, select the protocol you want: **RIP1, RIP1-Compatible, or RIP2**. If you don't want to transmit RIP messages, select **None**.

Static Routing

If the Gateway is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. To create a static route, change the following settings:

- Select Entry. Select the number of the static route from the drop-down menu. The Gateway supports up to 20 static route entries. If you need to delete a route, after selecting the entry, click the **Delete Entry** button.
- Destination IP Address. The Destination IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.
- Subnet Mask. The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.
- Hop Count. This determines the maximum number of steps between network nodes that data packets will travel. A node is any router in the path to the remote network.

- Interface. Select **LAN & Wireless** or **Internet**, depending on the location of the static route's final destination.
- Show Routing Table. Click the **Show Routing Table** button to open a screen (see Figure 5-12) displaying how data is routed through your LAN. For each route, the Destination IP address, Subnet Mask, Gateway, and Interface are displayed. Click the **Refresh** button to update the information.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

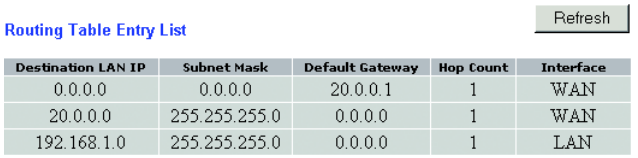

Figure 5-12: Routing Table

The Wireless Tab

Basic Wireless Settings (See Figure 5-13.)

This screen allows you to choose your wireless network mode and wireless security.

Wireless Network

- Wireless Network Mode. If you have 802.11g and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only 802.11g devices, select **802.11g**. If you have only 802.11b devices, select **802.11b**. If you want to disable wireless networking, select **Disabled**.
- Wireless Network Name (SSID). Enter the name for your wireless network into the field. The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Linksys recommends that you change the default SSID (linksys) to a unique name of your choice.
- Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly. Linksys wireless clients will automatically detect the wireless channel of the Gateway.

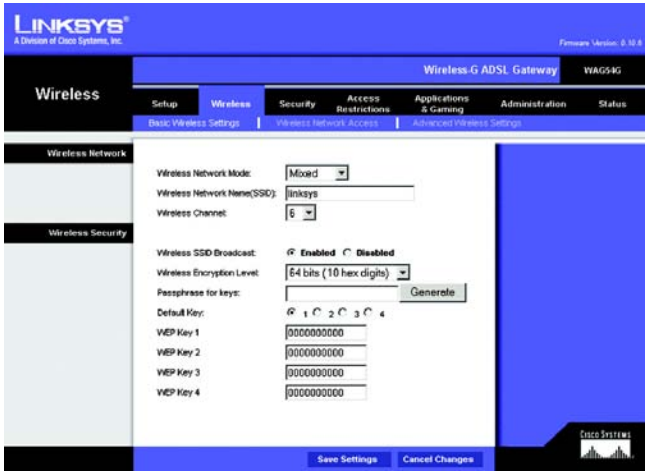

Figure 5-13: 64-Bit WEP Encryption

Wireless Security

- Wireless SSID Broadcast. When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Gateway. To broadcast the Gateway's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Gateway's SSID, then select **Disabled**.
- WEP Encryption Level. An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode data transmissions, all devices in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance. To enable WEP, select **64 bits (10 hex digits)** (see Figure 5-13) or **128 bits (26 hex digits)** (see Figure 5-14). To disable WEP encryption, keep the default setting, **No Encryption**.
- Passphrase for keys. Instead of manually entering WEP keys, you can enter a passphrase. This passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used

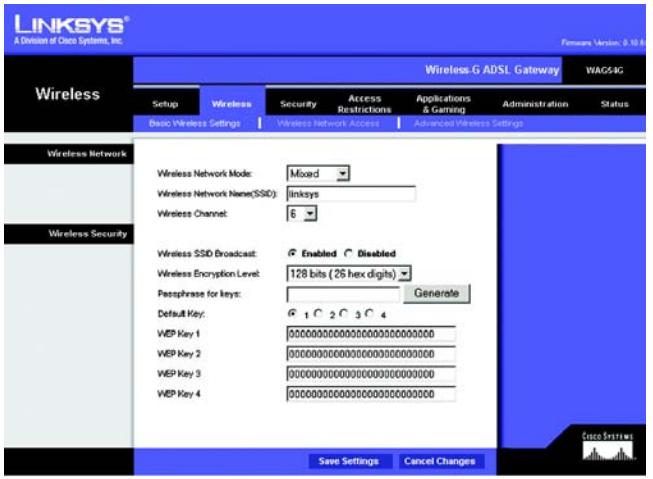

Figure 5-14: 128-Bit WEP Encryption

with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP key generated in the Key 1 field, and enter it manually in the wireless client.) After you enter the Passphrase, click the **Generate** button to create WEP keys.

- Default Key Select which WEP key (1-4) will be used when the Gateway sends data. Make sure that the receiving device (wireless client) is using the same key.
- WEP Keys 1-4. WEP keys enable you to create an encryption scheme for wireless network transmissions. If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.)

  If you are using 64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, the key must be exactly 26 hexadecimal characters in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Wireless Network Access (See Figure 5-15.)

Wireless Network Access. If you select **Allow All**, all computers will be allowed access to the wireless network. To restrict access to the network, select **Restrict Access to Computers below**. Click the **Select MAC Address From Networked Computers** button, and the screen in Figure 5-16 will appear.

Select the **MAC Address** from the list and click the **Select** box, then click the **Select** button.

Click the **Refresh** button if you want to refresh the screen. Click the **Close** button to return to the previous screen.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

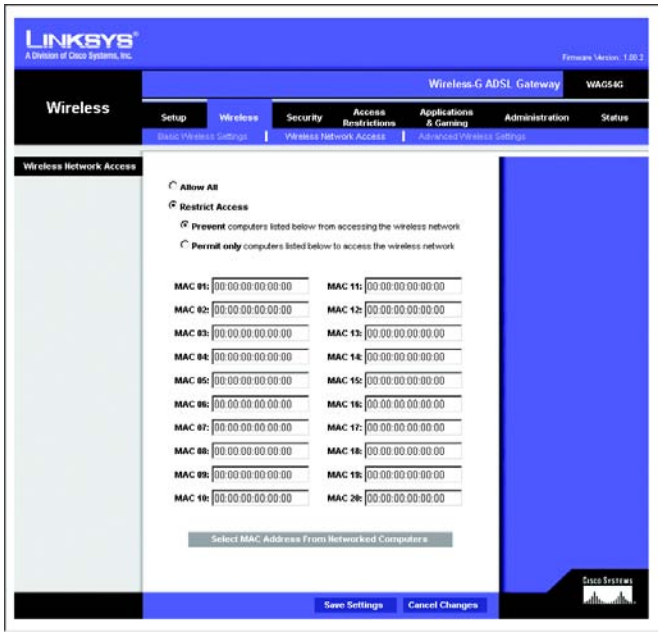

Figure 5-15: Wireless Network Access

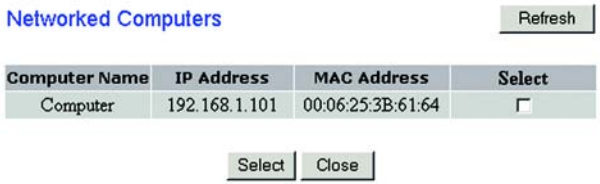

Figure 5-16: Networked Computers

Advanced Wireless Settings (See Figure 5-17.)

On this screen you can access the Advanced Wireless features, including Authentication Type, Basic Data Rates, Control Tx Rates, Beacon Interval, DTIM Interval, RTS Threshold, and Fragmentation Threshold.

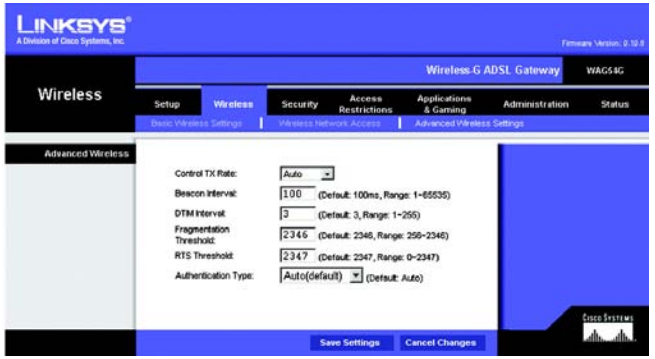

Figure 5-17: Advanced Wireless Settings

- Control Tx Rates. The default transmission rate is Auto. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, **Auto**, to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client.

- Beacon Interval. The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network.

- DTIM Interval. The default value is 3. This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

- Fragmentation Threshold. This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

- RTS Threshold. This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

- Authentication Type. The default is set to Auto (default), which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and the recipient do not use a WEP key for authentication but can use WEP for data encryption. If you want to allow on Open System authentication, then select **Open System**. For Shared Key authentication, the sender and recipient use a WEP key for both authentication and data encryption. If you want to use only Shared Key authentication, then select **Shared Key**. It is recommended that this option be left in the default (Auto) mode, because some clients cannot be configured for Shared Key.

The Security Tab

Firewall

When you click the Security tab, you will see the Firewall screen (see Figure 5-18). This screen contains Filters and the option to Block WAN Requests. Filters block specific Internet data types and block anonymous Internet requests.

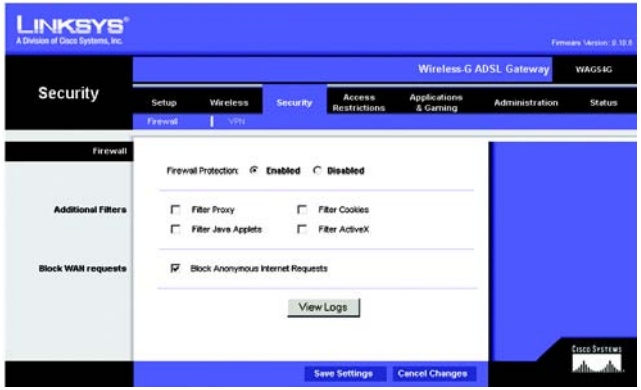

Figure 5-18: Firewall

- Firewall. To add Firewall Protection, click **Enabled**. If you do not want Firewall Protection, click **Disabled**.

  Additional Filters

- Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click **Enabled**.
- Filter Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click **Enabled**.
- Filter Java Applets. Java is a programming language for websites. If you deny Java Applets, you run the risk of not having access to Internet sites created using this programming language. To enable Java Applet filtering, click **Enabled**.
- Filter ActiveX. ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click **Enabled**.

  Block WAN requests

- Block Anonymous Internet Requests. This keeps your network from being “pinged” or detected and reinforces your network security by hiding your network ports, so it is more difficult for intruders to discover your network. Select **Block Anonymous Internet Requests** to block anonymous Internet requests or de-select it to allow anonymous Internet requests.

Click **View Logs** to view a log of any firewall events.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. The VPN screen, shown in Figure 5-19, allows you to configure your VPN settings to make your network more secure.

VPN Passthrough

- IPSec Passthrough. Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the **Enabled** button. To disable IPSec Passthrough, click the **Disabled** button.
- PPTP Passthrough. Point-to-Point Tunneling Protocol Passthrough is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP Passthrough, click the **Enabled** button. To disable PPTP Passthrough, click the **Disabled** button.

IPSec VPN Tunnel

The VPN Gateway creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure.

- To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to five simultaneous tunnels. Then click **Enabled** to enable the IPSec VPN tunnel. Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
- Local Secure Group and Remote Secure Group. The Local Secure Group is the computer(s) on your LAN that can access the tunnel. The Remote Secure Group is the computer(s) on the remote end of the tunnel that can access the tunnel. These computers can be specified by a Subnet, specific IP address, or range.
- Remote Security Gateway. The Remote Security Gateway is the VPN device, such as a second VPN Gateway, on the remote end of the VPN tunnel. Enter the IP Address or Domain of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Gateway, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local VPN Gateway, but the IP Address of the remote VPN Gateway or device with which you wish to communicate. If you enter an IP address, only the specific IP Address will be able to access the tunnel. If you select **Any**, any IP Address can access the tunnel.

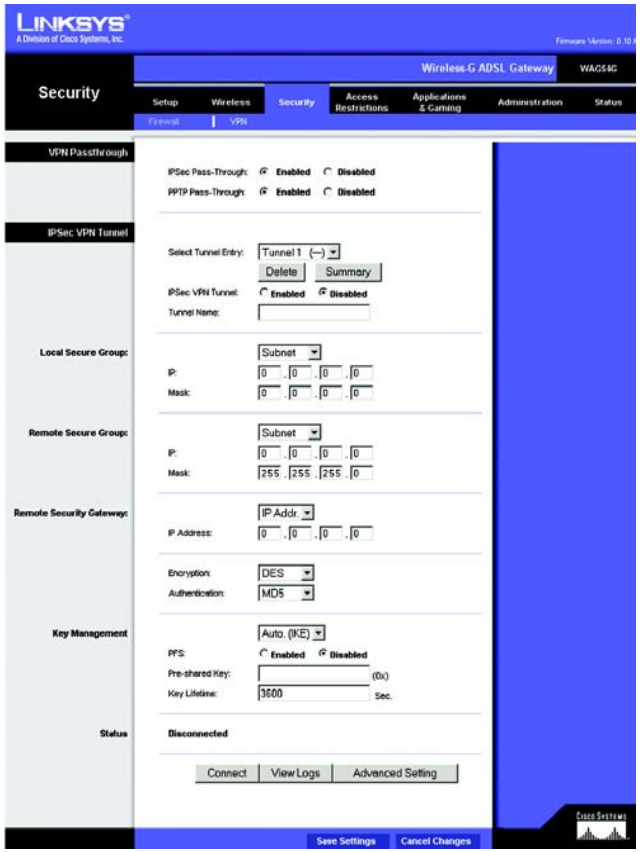

Figure 5-19: VPN

- Encryption. Using Encryption also helps make your connection more secure. There are two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable. In Figure 5-19, DES (which is the default) has been selected.

- Authentication. Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, if the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication. In Figure 5-19, MD5 (the default) has been selected.

- Key Management. Select **Auto (IKE)** or **Manual** from the drop-down menu. The two methods are described below.Auto (IKE)
  Select **Auto (IKE)** and enter a series of numbers or letters in the Pre-shared Key field. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may select to have the key expire at the end of a time period. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure.

  Manual (See Figure 5-20.)
  Select **Manual,** then select the Encryption Algorithm from the drop-down menu. Enter the Encryption Key in the field (if you chose DES for your Encryption Algorithm, enter 16 hexadecimal characters, if you chose 3DES, enter 48 hexadecimal characters). Select the Authentication Algorithm from the drop-down menu. Enter the Authentication Key in the field (if you chose MD5 for your Authentication Algorithm, enter 32 hexadecimal characters, if you chose SHA1, enter 40 hexadecimal characters). Enter the Inbound and Outbound SPIs in the respective fields.

- Status. The status of the connection is shown.

Click the **Connect** button to connect your VPN tunnel. Click the View Logs button to view logs. Click the **Advanced Setting** button and the Advanced IPSec VPN Tunnel Setup screen will appear. See Figure 5-20.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

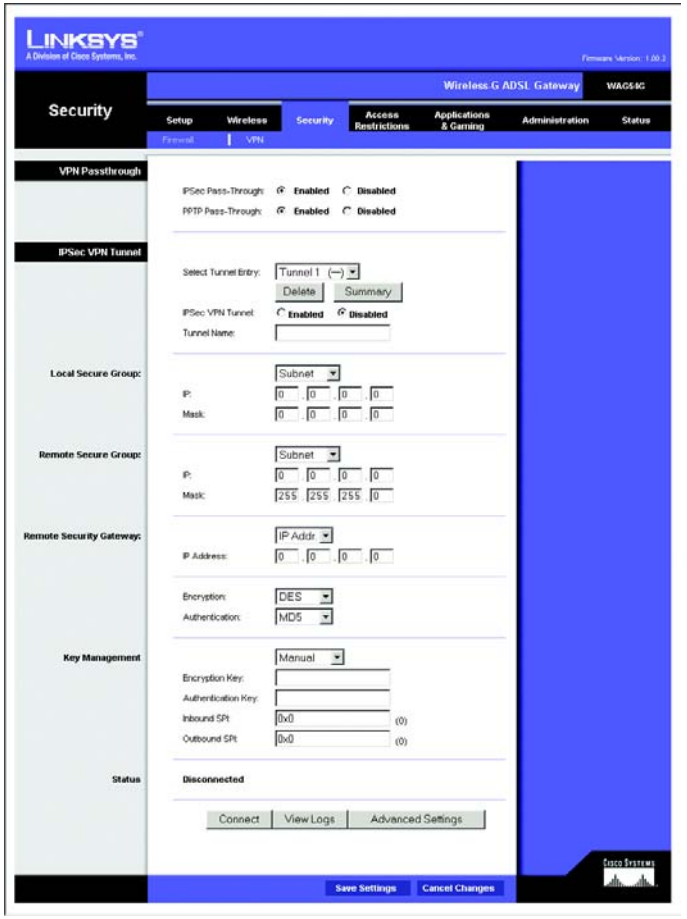

Figure 5-20: Manual Key Management

Advanced VPN Tunnel Setup

From the Advanced IPSec VPN Tunnel Setup screen, shown in Figure 5-21, you can adjust the settings for specific VPN tunnels.

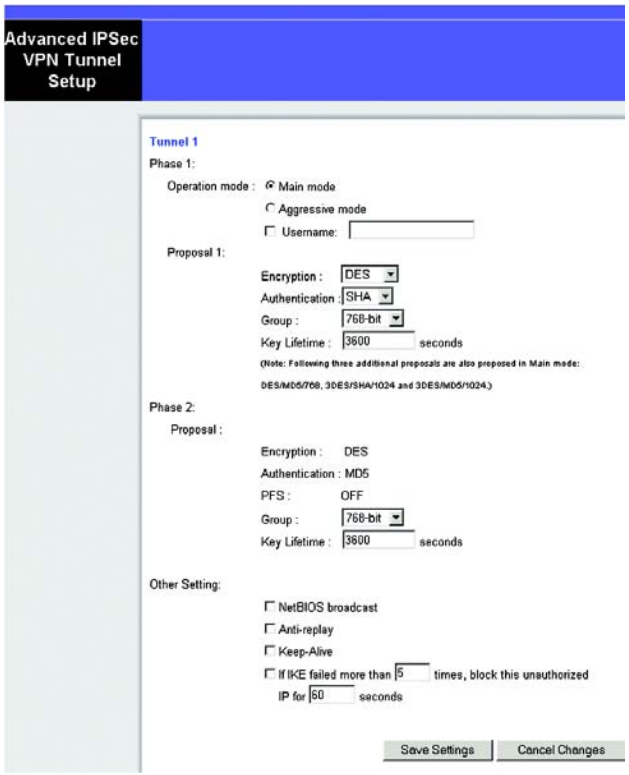

Figure 5-21: Advanced VPN Tunnel Setup

Phase 1

- Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.
- Operation Mode. There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Gateway will accept both Main and Aggressive requests from the remote VPN device. Select Username, then enter the user name.
- Encryption. Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.
- Authentication. Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.
- Key Life Time. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

- Encryption. The encryption method selected in Phase 1 will be displayed.
- Authentication. The authentication method selected in Phase 1 will be displayed.
- PFS. The status of PFS will be displayed.
- Group. There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

- Key Life Time. In the Key Lifetime field, you may select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Setting

- NetBIOS broadcast. Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel.
- Anti-replay. Check the box next to Anti-replay to enable the Anti-replay protection. This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level.
- Keep-Alive. If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection.
- Check this box to block unauthorized IP addresses. Enter in the field to specify how many times IKE must fail before blocking that unauthorized IP address. Enter the length of time that you specify (in seconds) in the field.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes. For further help on this tab, click the **Help** button.

The Access Restrictions Tab

Internet Access

The Access Restrictions tab, shown in Figure 5-22, allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific computers and set up filters by using network port numbers.

- Internet Access Policy. Multiple Filters can be saved as Internet Access Policies. When you wish to edit one, select the number of the Policy from the drop-down menu. The tab will change to reflect the settings of this Policy. If you wish to delete this Policy, click the **Delete** button. To see a summary of all Policies, click the **Summary** button.

  The summaries are listed on this screen, shown in Figure 5-23, with their name and settings. To return to the Filters tab, click the **Close** button.

- Enter Policy Name. Policies are created from the fields presented here.

  To create an Internet Access policy:

1. Enter a Policy Name in the field provided. Select **Internet Access** as the Policy Type.
2. Click the **Edit List** button. This will open the List of computers screen, shown in Figure 5-24. From this screen, you can enter the IP address or MAC address of any computer to which this policy will apply. You can even enter ranges of computers by IP address. Click the **Apply** button to save your settings, the **Cancel** button to undo any changes, and the **Close** button to return to the Filters tab.
3. If you wish to Deny or Allow Internet access for those computers you listed on the List of PCs screen, click the option.
4. You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting a service from the drop-down menus next to Blocked Services. If a service isn't listed, you can click the **Add/ Edit Service** button to open the Port Service screen, shown in Figure 5-25, and add a service to the list. You will need to enter a Service name, as well as the Protocol and Port Range used by the service.
5. By selecting the appropriate setting next to Days and Time, choose when Internet access will be filtered.
6. Click the **Save Settings** button to activate the policy.

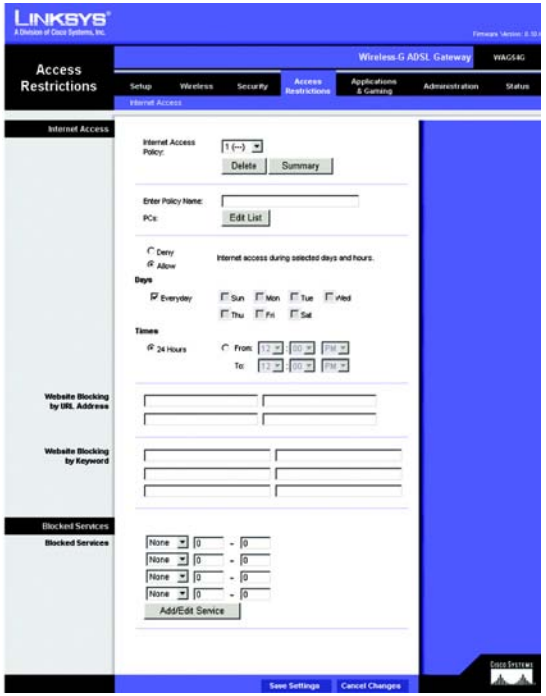

Figure 5-22: Access Restriction

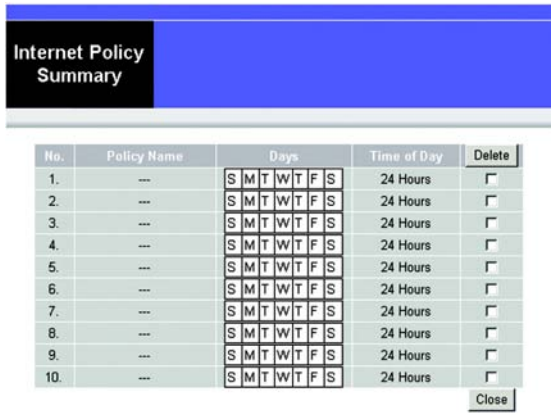
Internet Policy Summary
No.
Policy Name
Days
Time of Day
Delete
1. --- S M T W T F S 24 Hours
2. --- S M T W T F S 24 Hours
3. --- S M T W T F S 24 Hours
4. --- S M T W T F S 24 Hours
5. --- S M T W T F S 24 Hours
6. --- S M T W T F S 24 Hours
7. --- S M T W T F S 24 Hours
8. --- S M T W T F S 24 Hours
9. --- S M T W T F S 24 Hours
10. --- S M T W T F S 24 Hours
Close

Figure 5-23: Internet Policy Summary

Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the Website Blocking by URL Address fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

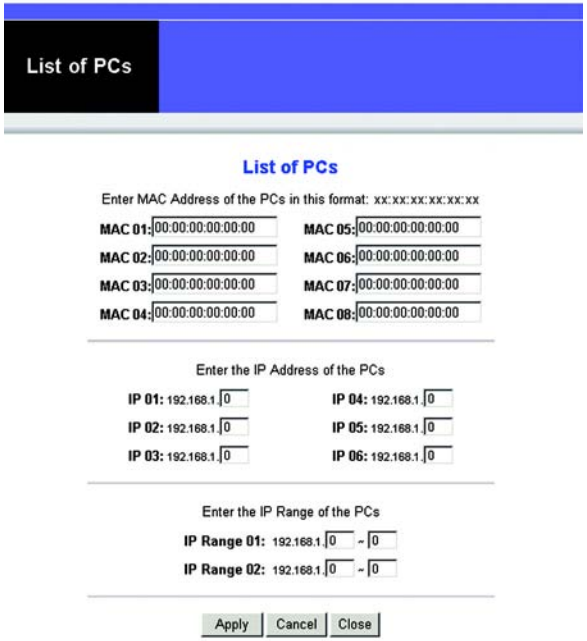

Figure 5-24: List of PCs

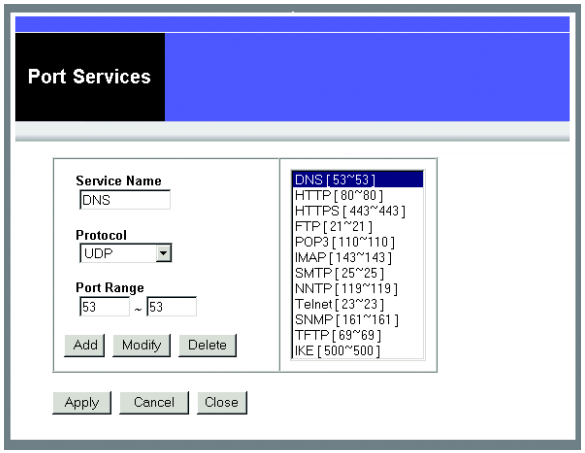

Figure 5-25: Port Services

The Applications and Gaming Tab

Single Port Forwarding

The Single Port Forwarding screen provides options for customization of port services for common applications. (See Figure 5-26.)

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Choose or enter the Application in the field. Then, enter the External and Internal Port numbers in the fields. Select the type of protocol you wish to use for each application: **TCP** or **UDP**. Enter the IP Address in the field. Click **Enabled** to enable UPnP Forwarding for the chosen application.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

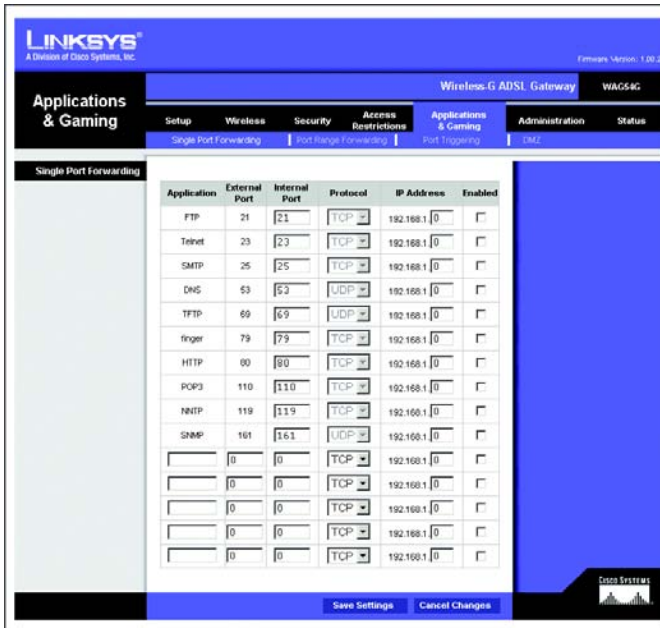

Figure 5-26: Single Port Forwarding

Port Range Forwarding

The Port Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) (See Figure 5-27.)

When users send this type of request to your network via the Internet, the Gateway will forward those requests to the appropriate computer. Any computer whose port is being forwarded should have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

- Application. Enter the name you wish to give each application.
- Start and End. Enter the starting and ending numbers of the port you wish to forward.
- TCP UDP. Select the type of protocol you wish to use for each application: **TCP**, **UDP**, or **Both**.
- IP Address. Enter the IP Address and Click **Enabled**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

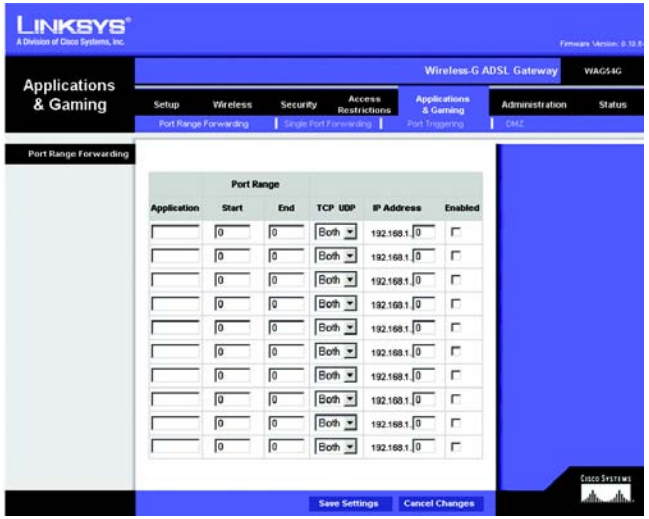

Figure 5-27: Port Range Forwarding

Port Triggering

Port Triggering is used for special applications that can request a port to be opened on demand. For this feature, the Gateway will watch outgoing data for specific port numbers. (See Figure 5-28.) The Gateway will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.

- Application. Enter the name you wish to give each application.
- Start Port and End Port. Enter the starting and ending Outgoing Triggered Range numbers and the Incoming Forwarded Range numbers of the port you wish to forward.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

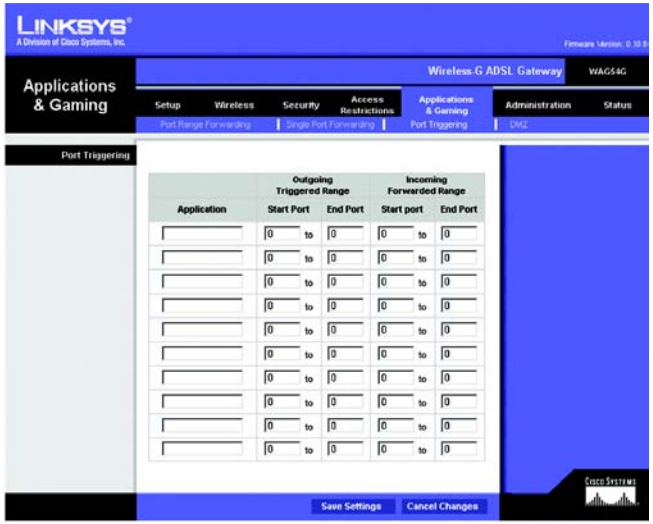

Figure 5-28: Port Triggering

DMZ

The DMZ screen (see Figure 5-29) allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing through DMZ Hosting. DMZ hosting forwards all the ports for one computer at the same time, which differs from Port Range Forwarding, which can only forward a maximum of 10 ranges of ports.

- DMZ Hosting. This feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming and videoconferencing. To use this feature, select **Enabled**. To disable DMZ, select **Disabled**.
- DMZ Host IP Address. To expose one computer, enter the computer's IP address. To get the IP address of a computer, refer to "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter."

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

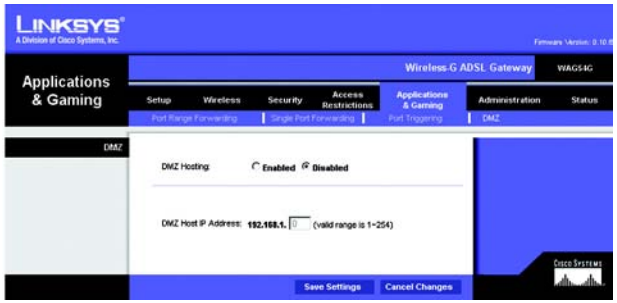

Figure 5-29: DMZ

The Administration Tab

Management

The Management screen, shown in Figure 5-30, allows you to change the Gateway's access settings as well as configure the SNMP (Simple Network Management Protocol) and UPnP (Universal Plug and Play) features.

Figure 5-30: Management

Gateway Access

Local Gateway Access. To ensure the Gateway's security, you will be asked for your password when you access the Gateway's Web-based Utility. The default username and password is admin.

- Gateway Username. Enter the default **admin**. It is recommended that you change the default username to one of your choice.
- Gateway Password. It is recommended that you change the default password to one of your choice.
- Re-enter to confirm. Re-enter the Gateway's new Password to confirm it.

Remote Gateway Access. This feature allows you to access the Gateway from a remote location, via the Internet.

IMPORTANT: Enabling remote Administration allows anyone with access to your password to configure the Gateway from somewhere else on the Internet.

- Remote Administration. This feature allows you to manage the Gateway from a remote location via the Internet. To enable Remote Administration, click **Enabled**.
- Administration Port. Enter the port number you will use to remotely access the Gateway.

SNMP

SNMP is a popular network monitoring and management protocol.

Identification. To enable SNMP, click **Enabled**. To disable SNMP, click **Disabled**.

- In the Device Name field, enter the name of the Gateway.
- Get Community. Enter the password that allows read-only access to the Gateway's SNMP information.

- Set Community. Enter the password that allows read/write access to the Gateway's SNMP information.

UPnP

UPnP allows Windows XP to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

UPnp. To enable UPnP, click **Enabled**.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Reporting

The Reporting tab, shown in Figure 5-31, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection. It also provides logs for VPN and firewall events.

Figure 5-31: Reporting

Log

Log. To enable log reporting, click **Enabled**.

- Logviewer IP Address. Enter the IP Address to receive logs into the field.

Email Alerts

E-Mail Alerts. To enable E-Mail Alerts, click **Enabled**.

- Denial of Service Thresholds. Enter the thresholds of events you want to receive.
- SMTP Mail Server. Enter the IP Address of the SMTP server in the field.
- E-Mail Address for Alert Logs. Enter the e-mail address for alert logs in the field.
- Return E-Mail address. Enter the address for the return e-mail.

To view the logs, click the **View Logs** button.

When finished making your changes on this tab, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Diagnostics

Ping Test (See Figure 5-32.)

Ping Test Parameters

- Ping Target IP. Enter the IP Address that you want to ping in the field. This can be either a local (LAN) IP or an Internet (WAN) IP address.
- Ping Size. Enter the size of the ping packets.
- No. of Pings. Enter the number of times that you want to ping.
- Ping Interval. Enter the ping interval in milliseconds.
- Ping Timeout. Enter the time in milliseconds.
- Ping Result. The results of the ping test will be shown here.

Click the **Start Test** button to start the Ping Test.

Figure 5-32: Ping Test

Factory Defaults (See Figure 5-33.)

Restore Factory Defaults. If you have exhausted all other options and wish to restore the Gateway to its factory default settings and lose all your settings, click **Yes**.

To begin the restore process, click the **Save Settings** button to save these changes, or click the **Cancel Changes** button to undo your changes.

Figure 5-33: Factory Defaults

Firmware Upgrade (See Figure 5-34.)

To upgrade the Gateway's firmware:

1. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys international website and then extracted.

2. Double-click the firmware file you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

Figure 5-34: Firmware Upgrade

The Status Tab

Gateway

This screen displays information about your Gateway and its WAN (Internet) Connections. (See Figure 5-35.)

Gateway Information

Gateway Information displays the Software Version, MAC Address, and Current Time.

Internet Connections

The Internet Connections displayed are the ADSL Link, PPP Login, Internet IP Address, Public Subnet Mask, Default Gateway, Primary DNS Server, and Internet DHCP IP Expires.

System Statistics

System Statistics displays the Packets Sent and Packets Received.

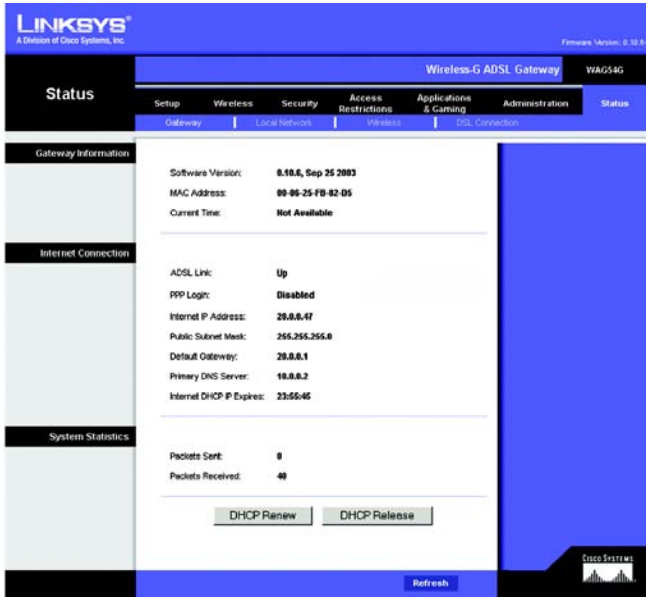

Figure 5-35: Status

DHCP Renew. Click the **DHCP Renew** button to replace your Gateway's current IP address with a new IP address.

DHCP Release. Click the **DHCP Release** button to delete your Gateway's current IP address.

Click the **Refresh** button if you want to Refresh your screen.

Local Network

The Local Network information that is displayed is the Local Mac Address, IP Address, Subnet Mask, and DHCP Server. To view the DHCP Clients Table, click the **DHCP Clients** button. See Figure 5-36.

DHCP Clients Table. Click the **DHCP Clients Table** button to show the current DHCP Client data. You will see the MAC address, computer name, and IP address of the network clients using the DHCP server. (This data is stored in temporary memory and changes periodically.) See Figure 5-37.

Click the **Refresh** button if you want to Refresh your screen.

Figure 5-36: Local Network

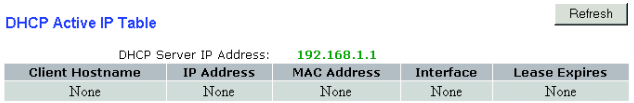

Figure 5-37: DHCP Clients Table

Wireless

The Wireless network information that is displayed is the Wireless Firmware Version, MAC Address, Status, Mode, Channel, SSID, and Encryption. (See Figure 5-38.)

Click the **Wireless Clients Connected** button to view the wireless clients connected to the Gateway.

Click the **Refresh** button if you want to Refresh your screen.

Figure 5-38: Wireless

DSL Connection

The DSL Connection information that is displayed is the Status, Downstream Rate, Upstream Rate, Encapsulation, VPI, VCI, and Multiplexing. (See Figure 5-40.)

Click the **Refresh** button if you want to Refresh your screen.

Figure 5-39: DSL Connection

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems that may occur during the installation and operation of the Gateway. Read the descriptions below to help you solve your problems. If you can't find an answer here, check the Linksys international website at www.linksys.com/international.

Common Problems and Solutions

1. I need to set a static IP address on a computer.

You can assign a static IP address to a computer by performing the following steps:

- For Windows 98 and Me:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.
  2. In The following network components are installed box, select the TCP/IP-> associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the Properties button.
  3. In the TCP/IP properties window, select the IP address tab, and select Specify an IP address. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway. Make sure that each IP address is unique for each computer or network device.
  4. Click the **Gateway** tab, and in the New Gateway prompt, enter 192.168.1.1, which is the default IP address of the Gateway. Click the Add button to accept the entry.
  5. Click the **DNS** tab, and make sure the DNS Enabled option is selected. Enter the Host and Domain names (e.g., John for Host and home for Domain). Enter the DNS entry provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.
  6. Click the **OK** button in the TCP/IP properties window, and click Close or the OK button for the Network window.
  7. Restart the computer when asked.
- For Windows 2000:
  1. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
  2. Right-click the Local Area Connection that is associated with the Ethernet adapter you are using, and select the Properties option.
  3. In the Components checked are used by this connection box, highlight Internet Protocol (TCP/IP), and click the **Properties** button. Select **Use the following IP address** option.
  4. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  5. Enter the Subnet Mask, 255.255.255.0.
  6. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).

7. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
8. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window, and click the **OK** button in the Local Area Connection Properties window.
9. Restart the computer if asked.

- For Windows XP:
  The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.
  1. Click **Start** and **Control Panel**.
  2. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
  3. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the Properties option.
  4. In the **This connection uses the following items** box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
  5. Enter a unique IP address that is not used by any other computer on the network connected to the Gateway.
  6. Enter the Subnet Mask, 255.255.255.0.
  7. Enter the Default Gateway, 192.168.1.1 (Gateway's default IP address).
  8. Toward the bottom of the window, select Use the following DNS server addresses, and enter the Preferred DNS server and Alternative DNS server (provided by your ISP). Contact your ISP or go on its website to find the information.
  9. Click the **OK** button in the Internet Protocol (TCP/IP) Properties window. Click the **OK** button in the Local Area Connection Properties window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 98, Me, 2000, and XP:

- Refer to "Chapter 4: Configure the computers" for details. Make sure Obtain IP address automatically is selected in the settings.

For Windows NT 4.0:

- Click **Start**, **Setting**s, and **Control Panel**. Double-click the **Network** icon.
- Click the Protocol tab, and double-click on TCP/IP Protocol.
- When the window appears, make sure you have selected the correct Adapter for your Ethernet adapter and set it for **Obtain an IP address** from a DHCP server.
- Click the **OK** button in the TCP/IP Protocol Properties window, and click the **Close** button in the Network window.
- Restart the computer if asked.

B. Open a command prompt.

For Windows 98 and Me:

- Click **Start** and **Run**. In the Open field, type in command. Press the **Enter** key or click the **OK** button.

For Windows NT, 2000, and XP:

- Click **Start** and **Run**. In the Open field, type cmd. Press the **Enter** key or click the **OK** button. In the command prompt, type ping 192.168.1.1 and press the Enter key.
- If you get a reply, the computer is communicating with the Gateway.
- If you do NOT get a reply, please check the cable, and make sure Obtain an IP address automatically is selected in the TCP/IP settings for your Ethernet adapter.

C. In the command prompt, type ping followed by your Internet or WAN IP address and press the **Enter** key. The Internet or WAN IP Address can be found on the Status screen of the Gateway's web-based utility. For example, if your Internet or WAN IP address is 1.2.3.4, you would enter ping 1.2.3.4 and press the Enter key.

- If you get a reply, the computer is connected to the Gateway.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

D. In the command prompt, type ping www.yahoo.com and press the **Enter** key.

- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the Internet with my Internet connection.

- Refer to "Problem #2, I want to test my Internet connection" to verify that you have connectivity.
  1. Make sure you are using the right Internet connection settings. Contact your ISP to see if your Internet connection type is RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, or RFC 2364 PPPoA. Please refer to the Setup section of "Chapter 5: Configuring the Gateway" for details on Internet connection settings.
  2. Make sure you have the right cable. Check to see if the Gateway column has a solidly lit ADSL LED.
  3. Make sure the cable connecting from your Gateway's ADSL port is connected to the wall jack of the ADSL service line. Verify that the Status page of the Gateway's web-based utility shows a valid IP address from your ISP.
  4. Turn off the computer and Gateway. Wait 30 seconds, and then turn on the Gateway, and computer. Check the Status tab of the Gateway's web-based utility to see if you get an IP address.

4. I am not able to access the Setup page of the Gateway's web-based utility.

- Refer to "Problem #2, I want to test my Internet connection" to verify that your computer is properly connected to the Gateway.
  1. Refer to "Appendix D: Finding the MAC Address and IP address for Your Ethernet Adapter" to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
  2. Set a static IP address on your system; refer to "Problem #1: I need to set a static IP address."

3. Refer to "Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users)."

5. I can't get my Virtual Private Network (VPN) working through the Gateway.

Access the Gateway's web interface by going to http://192.168.1.1 or the IP address of the Gateway, and go to the Security tab. Make sure you have IPsec passthrough and/or PPTP pass-through enabled.

- VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.
- VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Gateway. AH has limitations due to occasional incompatibility with the NAT standard.
- Change the IP address for the Gateway to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Gateway will have difficulties routing information to the right location. If you change the Gateway's IP address to 192.168.2.1, that should solve the problem. Change the Gateway's IP address through the Setup tab of the web interface.
- If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.
- Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.
- Check the Linksys international website for more information at www.linksys.com/international.

6. I need to set up a server behind my Gateway and make it available to the public.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed.

- Follow these steps to set up port forwarding through the Gateway's web-based utility. We will be setting up web, ftp, and mail servers.
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
  2. Enter any name you want to use for the Customized Application.
  3. Enter the External Port range of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
  4. Check the protocol you will be using, TCP and/or UDP.
  5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the

field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

6. Check the Enable option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X		192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X		192.168.1.102	X
POP3 (incoming)	110 to 110	X		192.168.1.102	X

When you have completed the configuration, click the **Save Settings** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Gateway to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

1. Access the Gateway's web interface by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => Port Range Forwarding tab.
2. Enter any name you want to use for the Customized Application.
3. Enter the External Port range of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
4. Check the protocol you will be using, TCP and/or UDP.
5. Enter the IP address of the computer or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
6. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	External Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Save Settings** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Gateway will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Gateway will send the data to whichever computer or network device you set for DMZ hosting.)

- Follow these steps to set DMZ hosting:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Go to the Applications and Gaming => DMZ tab. Click Enabled and enter the IP of the computer.
  2. Check the Port Forwarding pages and disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
- Once completed with the configuration, click the **Save Settings** button.

9. I forgot my password, or the password prompt always appears when I am saving settings to the Gateway.

- Reset the Gateway to factory default by pressing the Reset button for 10 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:
  1. Access the Gateway's web-based utility by going to http://192.168.1.1 or the IP address of the Gateway. Enter the default username and password **admin**, and click the **Administrations** => **Management** tab.
  2. Enter a different password in the Gateway Password field, and enter the same password in the second field to confirm the password.
  3. Click the **Save Settings** button.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Gateway is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

- For Microsoft Internet Explorer 5.0 or higher:
  1. Click **Start, Settings**, and **Control Panel**. Double-click Internet Options.
  2. Click the **Connections** tab.
  3. Click the **LAN settings** button and remove anything that is checked.
  4. Click the **OK** button to go back to the previous screen.
  5. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

- For Netscape 4.7 or higher:
  1. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
  2. Make sure you have Direct connection to the Internet selected on this screen.
  3. Close all the windows to finish.

11. To start over, I need to set the Gateway to factory default.

Hold the **Reset** button for 10 seconds and then release it. This will return the Internet settings, password, forwarding, and other settings on the Gateway to the factory default settings. In other words, the Gateway will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys international website and download the latest firmware at www.linksys.com/international.

- Follow these steps:
  1. Go to the Linksys international website at http://www.linksys.com/international and select your region or country.
  2. Click the **Products** tab and select the Gateway.
  3. On the Gateway's webpage, click **Firmware**, and then download the latest firmware for the Gateway.
  4. To upgrade the firmware, follow the steps in the Administration section found in "Chapter 5: Configuring the Gateway."

13. The firmware upgrade failed, and/or the Power LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Power LED stop flashing:

- If the firmware upgrade failed, use the TFTP program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.
- Set a static IP address on the computer; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:
  IP Address: 192.168.1.50
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1
- Perform the upgrade using the TFTP program or the Gateway's web-based utility through its Administration tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet.

- There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
2. Enter the username and password, if asked. (The default username and password is admin.)
3. On the Setup screen, select the option **Keep Alive**, and set the Redial Period option at 20 (seconds).
4. Click the **Save Settings** button. Click the **Status** tab, and click the **Connect** button.
5. You may see the login status display as Connecting. Press the F5 key to refresh the screen, until you see the login status display as Connected.
6. Click the **Save Settings** button to continue.

- If the connection is lost again, follow steps 1- 6 to re-establish connection.

15. I can't access my e-mail, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set automatically.

- If you are having some difficulties, perform the following steps:
  1. To connect to the Gateway, go to the web browser, and enter http://192.168.1.1 or the IP address of the Gateway.
  2. Enter the username and password, if asked. (The default username and password is admin.)
  3. Look for the MTU option, and select **Manual**. In the Size field, enter 1492.
  4. Click the **Save Settings** button to continue.
- If your difficulties continue, change the Size to different values. Try this list of values, one value at a time, in this order, until your problem is solved:
  1462
  1400
  1362
  1300

16. The Power LED flashes continuously.

The Power LED lights up when the device is first powered up. In the meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED remains steady to show that the system is working fine. If the LED continues to flash after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0.

17. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other computers work. If they do, ensure that your computer's IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and powered on. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)

- If the Gateway is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Gateway to verify a direct connection.
- Manually configure the TCP/IP settings with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

Frequently Asked Questions

What is the maximum number of IP addresses that the Gateway will support?
The Gateway will support up to 253 IP addresses.

Is IPSec Passthrough supported by the Gateway?
Yes, it is a built-in feature that is enabled by default.

Where is the Gateway installed on the network?
In a typical environment, the Gateway is installed between the ADSL wall jack and the LAN.

Does the Gateway support IPX or AppleTalk?
No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from the Internet to a LAN.

Does the LAN connection of the Gateway support 100Mbps Ethernet?
The Gateway supports 100Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Gateway.

What is Network Address Translation and what is it used for?
Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a computer connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Gateway to be used with low cost Internet accounts when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Gateway support any operating system other than Windows 98SE, Windows Millennium, Windows 2000, or Windows XP?
Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Gateway support ICQ send file?
Yes, with the following fix: click ICQ menu -> preference -> connections tab->, and check I am behind a firewall or proxy. Then set the firewall time-out to 80 seconds in the firewall setting. The Internet user can then send a file to a user behind the Gateway.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do?
If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port. (Port 8080 usually works well but is used for remote admin. You may have to disable this.) Then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Gateway from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address?
It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get Half-Life: Team Fortress to work with the Gateway?
The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. One problem: Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do?
Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at www.linksys.com/international for more information.

If all else fails in the installation, what can I do?
Reset the Gateway by holding down the reset button until the Power LED fully turns on and off. Reset your DSL modem by powering the unit off and then on. Obtain and flash the latest firmware release that is readily available on the Linksys international website, www.linksys.com/international.

How will I be notified of new Gateway firmware upgrades?
All Linksys firmware upgrades are posted on the Linksys international website at www.linksys.com/international, where they can be downloaded for free. To upgrade the Gateway's firmware, use the Administration tab of the

Gateway's web-based utility. If the Gateway's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use.

Will the Gateway function in a Macintosh environment?
Yes, but the Gateway's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Gateway. What can I do?
You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click Tools, Internet Options, and then the Connection tab. Make sure that Internet Explorer is set to Never dial a connection. For Netscape Navigator, click Edit, Preferences, Advanced, and Proxy. Make sure that Netscape Navigator is set to Direct connection to the Internet.

What is DMZ Hosting?
Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter."

If DMZ Hosting is used, does the exposed user share the public IP with the Gateway?
No.

Does the Gateway pass PPTP packets or actively route PPTP sessions?
The Gateway allows PPTP packets to pass through.

Is the Gateway cross-platform compatible?
Any platform that supports Ethernet and TCP/IP is compatible with the Gateway.

How many ports can be simultaneously forwarded?
Theoretically, the Gateway can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

What are the advanced features of the Gateway?
The Gateway's advanced features include Advanced Wireless settings, Filters, Port Forwarding, Routing, and DDNS.

What is the maximum number of VPN sessions allowed by the Gateway?
The maximum number depends on many factors. At least one IPSec session will work through the Gateway; however, simultaneous IPSec sessions may be possible, depending on the specifics of your VPNs.

How can I check whether I have static or DHCP IP Addresses?
Consult your ISP to obtain this information.

How do I get mIRC to work with the Gateway?
Under the Port Forwarding tab, set port forwarding to 113 for the computer on which you are using mIRC.

Can the Gateway act as my DHCP server?
Yes. The Gateway has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b and 802.11g features are supported?
The product supports the following IEEE 802.11b and IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other, peer-to-peer without the use of an access point.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

What is roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Will the information be intercepted while it is being transmitted through the air?
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

What is WEP?
WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?
The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Gateway?
Press the Reset button on the back panel for about ten seconds. This will reset the Gateway to its default settings.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Gateway and a wireless computer will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Gateway and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Gateway, but not on your wireless adapter (or vice versa). Verify that the same WEP keys and levels (64 or 128) are being used on all nodes of your wireless network.

How many channels/frequencies are available with the Gateway?
There are eleven available channels, ranging from 1 to 11 (in North America).

If your questions are not addressed here, refer to the Linksys international website, www.linksys.com/international.

Appendix B: Wireless Security

Important Information for Wireless Products

Linksys wants to make wireless networking as safe and easy for you as possible. So, please keep the following points in mind whenever setting up or using your wireless network.

1. Performance.

The actual performance of your wireless network depends on a number of factors, including:

In an Infrastructure environment, your distance from the access point. As you get farther away, the transmission speed will decrease.

Structural interference. The shape of your building or structure, the type of construction, and the building materials used may have an adverse impact on signal quality and speed.

The placement and orientation of the wireless devices.

2. Interference.

Any device operating in the 2.4 GHz spectrum may cause network interference with a 802.11b wireless device. Some devices that may prove troublesome include 2.4 GHz cordless phones, microwave ovens, adjacent public hotspots, and neighboring 802.11b wireless LANs.

3. Security.

The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation.

While the following is a complete list, steps A through E should, at least, be followed:

A. Change the default SSID.

B. Disable SSID Broadcasts.

C. Change the default password for the Administrator account.

D. Enable MAC Address Filtering.

E. Change the SSID periodically.

F. Enable WEP 128-bit Encryption. Please note that this will reduce your network performance.

G. Change the WEP encryption keys periodically.

For information on implementing these security features, please refer to the User Guide.

4. Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages are decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier) and the IP Address of the network PC or access point. Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

A. Disable Broadcast

B. Make it unique

C. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a panacea for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

A. Use the highest level of encryption possible

B. Use a "Shared" Key

C. Use multiple WEP keys

D. Change your WEP key regularly

Implementing encryption will have a negative impact on your network's performance. If you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Configuring IPSec between a Windows 2000 or XP Computer and the Gateway

Introduction

This document demonstrates how to establish a secure IPSec tunnel using preshared keys to join a private network inside the Gateway and a Windows 2000 or XP computer. You can find detailed information on configuring the Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

NOTE: Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Gateway's Web-Based Utility.

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP
IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

WAG54G

WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

How to Establish a Secure IPSec Tunnel

Step 1: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the **Open** field. The Local Security Setting screen will appear as shown in Figure C-1.
2. Right-click **IP Security Policies on Local Computer**, and click **Create IP Security Policy**.
3. Click the **Next** button, and then enter a name for your policy (for example, to_Gateway). Then, click **Next**.
4. Deselect the Activate the default response rule check box, and then click the **Next** button.
5. Click the **Finish** button, making sure the Edit check box is checked.

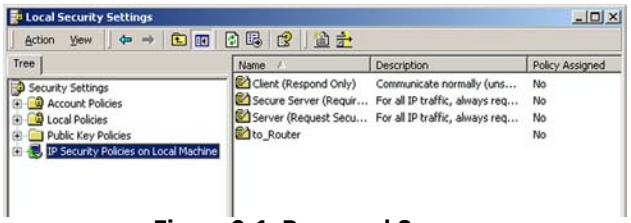

Figure C-1: Password Screen

NOTE: The references in this section to "win" are references to Windows 2000 and XP.

Step 2: Build Filter Lists

Filter List 1: win->Gateway

1. In the new policy's properties screen, verify that the Rules tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.
2. Make sure the IP Filter List tab is selected, and click the **Add** button. (See Figure C-3.)

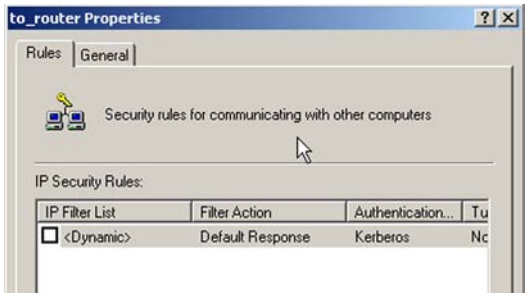

Figure C-2: Setup Tab

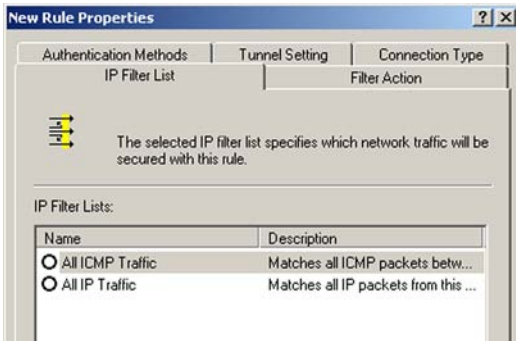

Figure C-3: IP Filter List Tab

3. The IP Filter List screen should appear, as shown in Figure C-4. Enter an appropriate name, such as win->Gateway, for the filter list, and de-select the Use **Add** Wizard check box. Then, click the **Add** button.

4. The Filters Properties screen will appear, as shown in Figure C-5. Select the Addressing tab. In the Source address field, select My IP Address. In the Destination address field, select A specific IP Subnet, and fill in the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (These are the Gateway's default settings. If you have changed these settings, enter your new values.)

5. If you want to enter a description for your filter, click the Description tab and enter the description there.

6. Click the **OK** button. Then, click the **OK** (for Windows XP) or **Close** (for Windows 2000) button on the IP Filter List window.

Filter List 2: Gateway=>win

7. The New Rule Properties screen will appear, as shown in Figure C-6. Select the IP Filter List tab, and make sure that **win -> Gateway** is highlighted. Then, click the **Add** button.

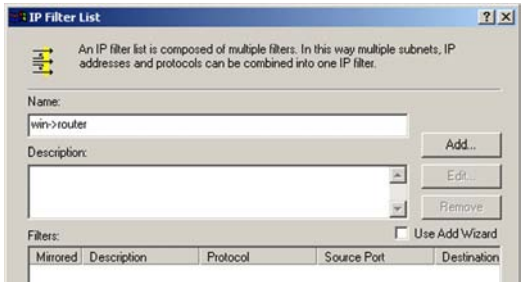

Figure C-4: IP Filter List

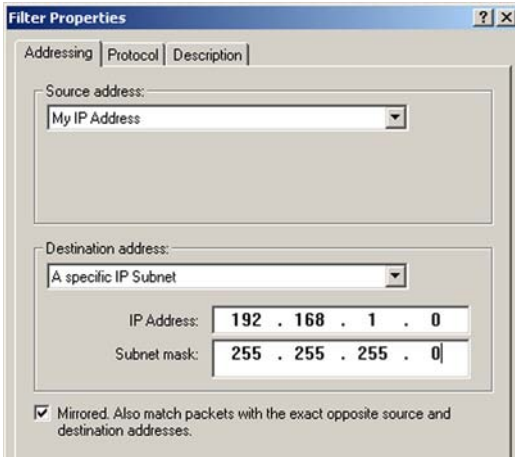

Figure C-5: Filters Properties

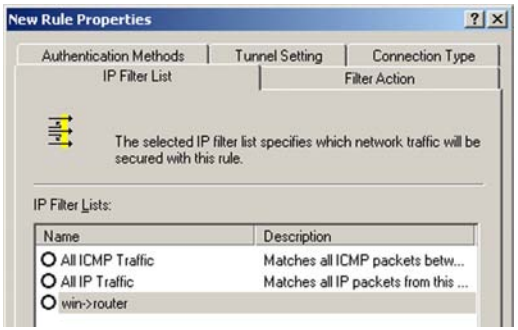

Figure C-6: New Rule Properties

8. The IP Filter List screen should appear, as shown in Figure C-7. Enter an appropriate name, such as Gateway->win for the filter list, and de-select the Use **Add Wizard** check box. Click the **Add** button.

9. The Filters Properties screen will appear, as shown in Figure C-8. Select the Addressing tab. In the Source address field, select **A specific IP Subnet**, and enter the IP Address: 192.168.1.0 and Subnet mask: 255.255.255.0. (Enter your new values if you have changed the default settings.) In the Destination address field, select My IP Address.

10. If you want to enter a description for your filter, click the Description tab and enter the description there.

11. Click the **OK** button and the New Rule Properties screen should appear with the IP Filer List tab selected, as shown in Figure C-9. There should now be a listing for "Gateway -> win" and "win -> Gateway". Click the **OK** (for WinXP) or **Close** (for Win2000) button on the IP Filter List window.

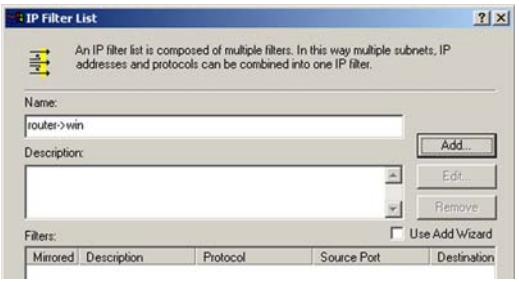

Figure C-7: IP Filter List

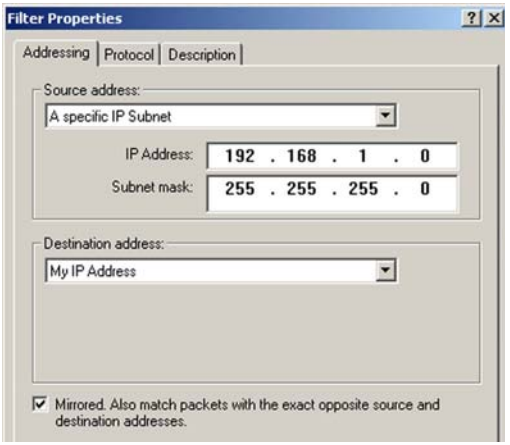

Figure C-8: Filters Properties

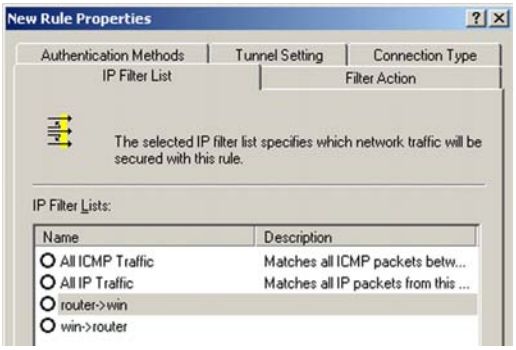

Figure C-9: New Rule Properties

Step 3: Configure Individual Tunnel Rules

Tunnel 1: win->Gateway

1. From the IP Filter List tab, shown in Figure C-10, click the filter list win->Gateway.
2. Click the **Filter Action** tab (as in Figure C-11), and click the filter action Require Security radio button. Then, click the Edit button.
3. From the Security Methods tab, shown in Figure C-12, verify that the Negotiate security option is enabled, and deselect the **Accept unsecured communication**, but always respond using IPSec check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.

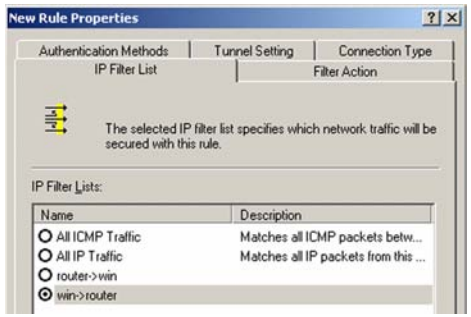

Figure C-10: IP Filter List Tab

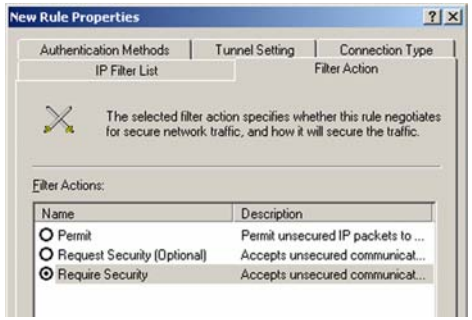

Figure C-11: Filter Action Tab

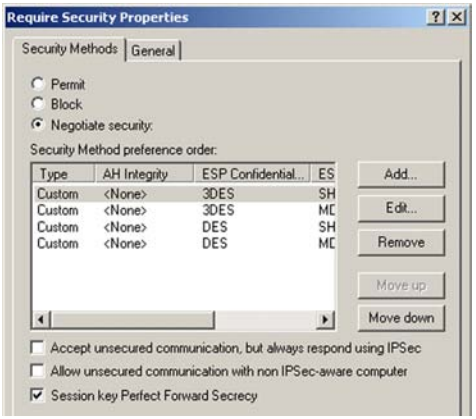

Figure C-12: Security Methods Tab

4. Select the **Authentication Methods** tab, shown in Figure C-13, and click the **Edit** button.

5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, as shown in Figure C-14, and enter the preshared key string, such as XYZ12345. Click the **OK** button.

6. This new Preshared key will be displayed in Figure C-15. Click the **OK** or **Close** button to continue.

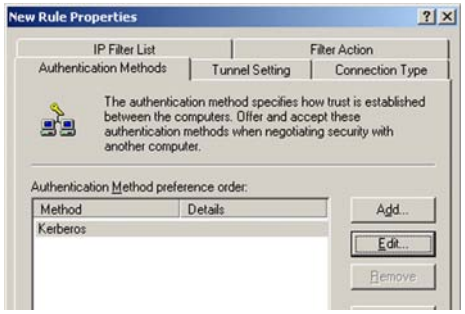

Figure C-13: Authentication Methods

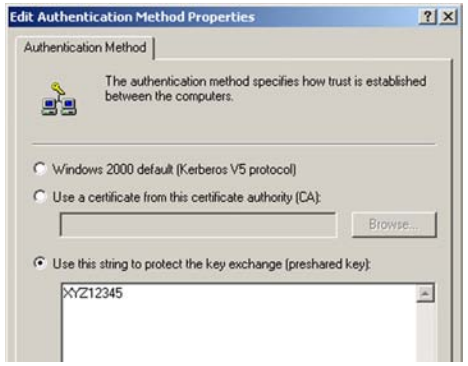
Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
XYZ12345

Figure C-14: Preshared Key

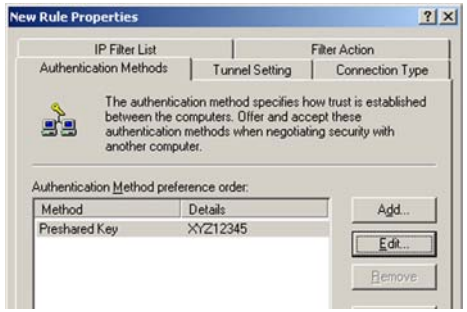

Figure C-15: New Preshared Key

7. Select the **Tunnel Setting** tab, shown in Figure C-16, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Gateway's WAN IP Address.

8. Select the **Connection Type** tab, as shown in Figure C-17, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.

Tunnel 2: Gateway->win

9. In the new policy's properties screen, shown in Figure C-18, make sure that "win -> Gateway" is selected and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.

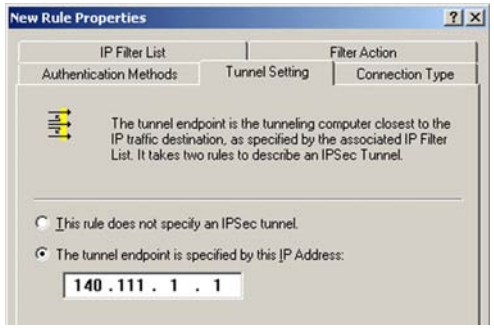
New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
140 . 111 . 1 . 1

Figure C-16: Tunnel Setting Tab

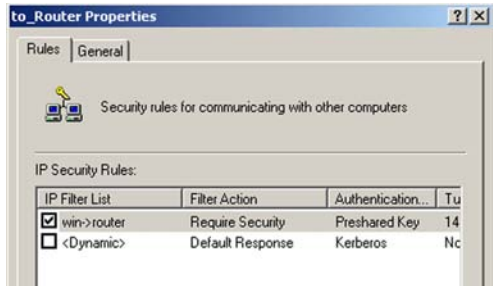

Figure C-17: Connection Type Tab

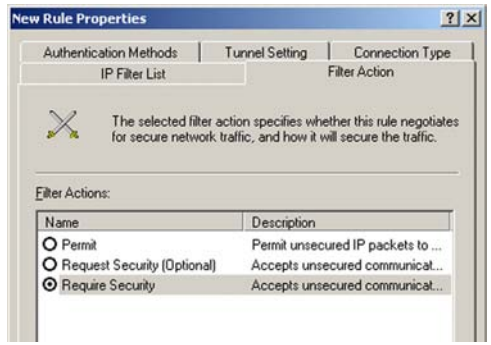

Figure C-18: Properties Screen

10. Go to the **IP Filter List** tab, and click **the filter list Gateway->win**, as shown in Figure C-19.

11. Click the **Filter Action** tab, and select the filter action **Require Security**, as shown in Figure C-20. Then, click the **Edit** button.

12. Click the **Authentication Methods** tab, and verify that the authentication method Kerberos is selected, as shown in Figure C-21. Then, click the **Edit** button.

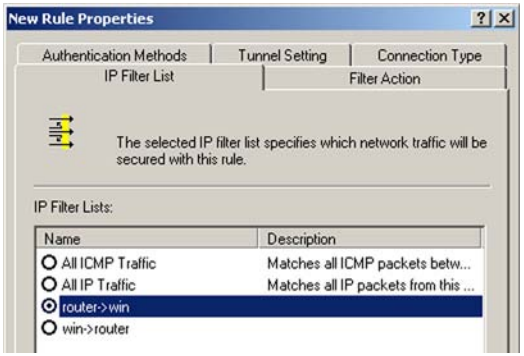

Figure C-19: IP Filter List Tab

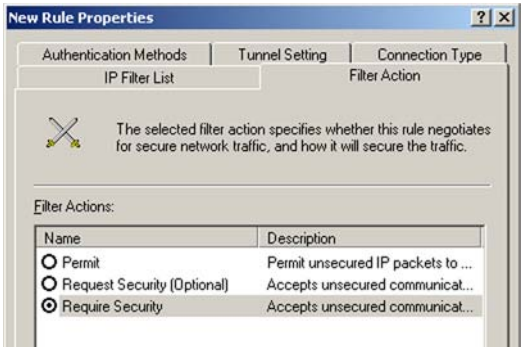

Figure C-20: Filter Action Tab

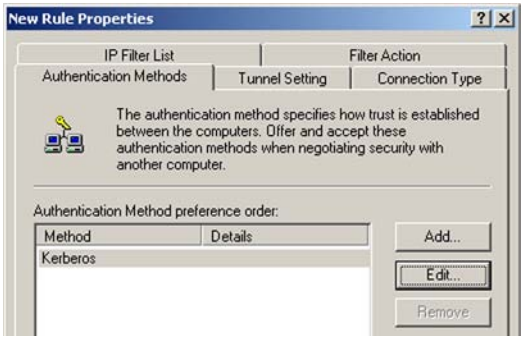

Figure C-21: Authentication Methods Tab

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as XYZ12345, as shown in Figure C-22. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.

14. This new Preshared key will be displayed in Figure C-23. Click the **OK** button to continue.

15. From the Tunnel Setting tab, shown in Figure C-24, click the radio button for **The tunnel endpoint is specified by this IP Address,** and enter the Windows 2000/XP computer's IP Address.

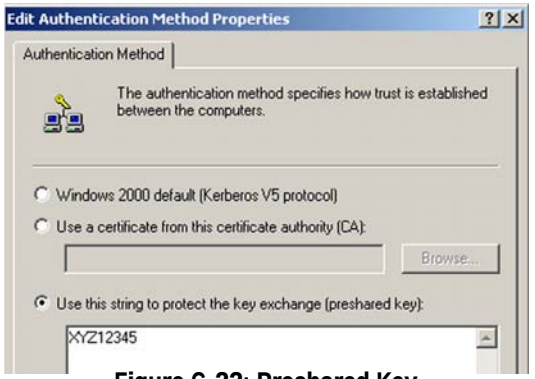
Edit Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this certificate authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
XYZ12345

Figure C-22: Preshared Key

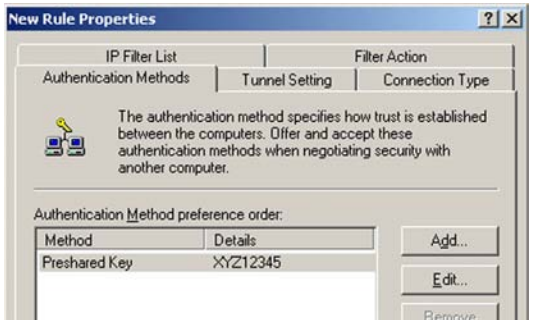

Figure C-23: New Preshared Key

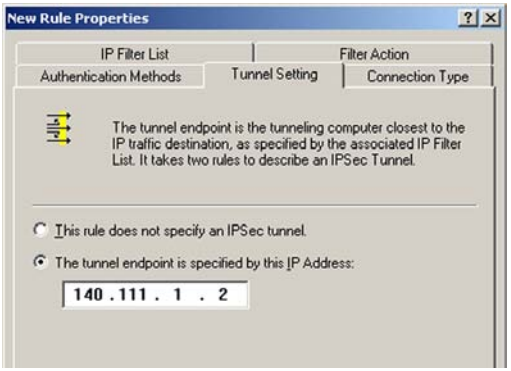
New Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.
This rule does not specify an IPSec tunnel.
The tunnel endpoint is specified by this IP Address:
140 . 111 . 1 . 2

Figure C-24: Tunnel Setting Tab

16. Click the **Connection Type** tab, shown in Figure C-25, and select **All network connections**. Then click the **OK** (for Windows XP) or **Close** (for Windows 2000) button to finish.

17. From the Rules tab, shown in Figure C-26, click the **OK** button to return to the secpol screen.

Step 4: Assign New IPSec Policy

In the IP Security Policies on Local Computer window, shown in Figure C-27, right-click the policy named to_Gateway, and click **Assign**. A green arrow appears in the folder icon.

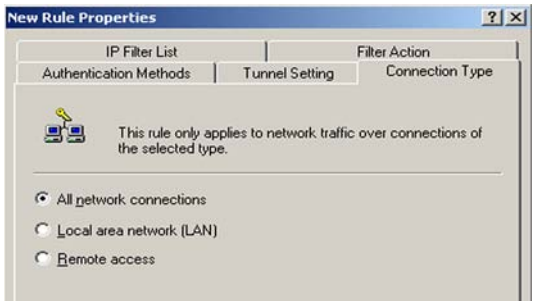

Figure C-25: Connection Type

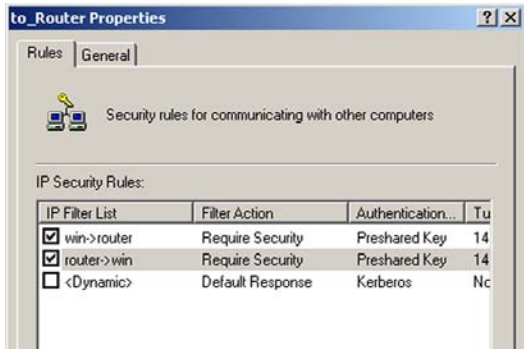

Figure C-26: Rules

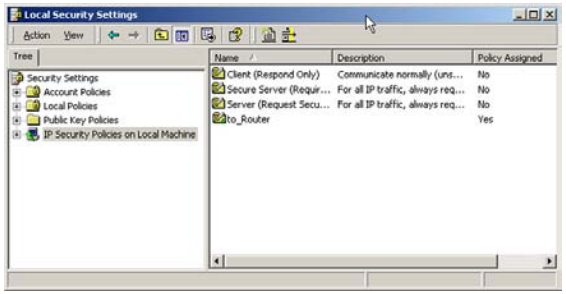

Figure C-27: Local Computer

Step 5: Create a Tunnel Through the Web-Based Utility

1. Open your web browser, and enter **192.168.1.1** in the Address field. Press the **Enter** key.
2. When the User name and Password field appears, enter the default the user name and password **admin**. Press the **Enter** key.
3. From the Setup tab, click the **VPN** tab.
4. From the VPN tab, shown in Figure C-28, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. Then click **Enabled**. Enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.
5. Enter the IP Address and Subnet Mask of the local VPN Gateway in the Local Secure Group fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Gateway or device with which you wish to communicate) in the Remote Security Gateway fields.
7. Select from two different types of encryption: DES or 3DES (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting Disable.
8. Select from two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication.
9. Select the Key Management. Select Auto (IKE) and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to PFS (Perfect Forward Secrecy) to ensure that the initial key exchange and IKE proposals are secure. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.
10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

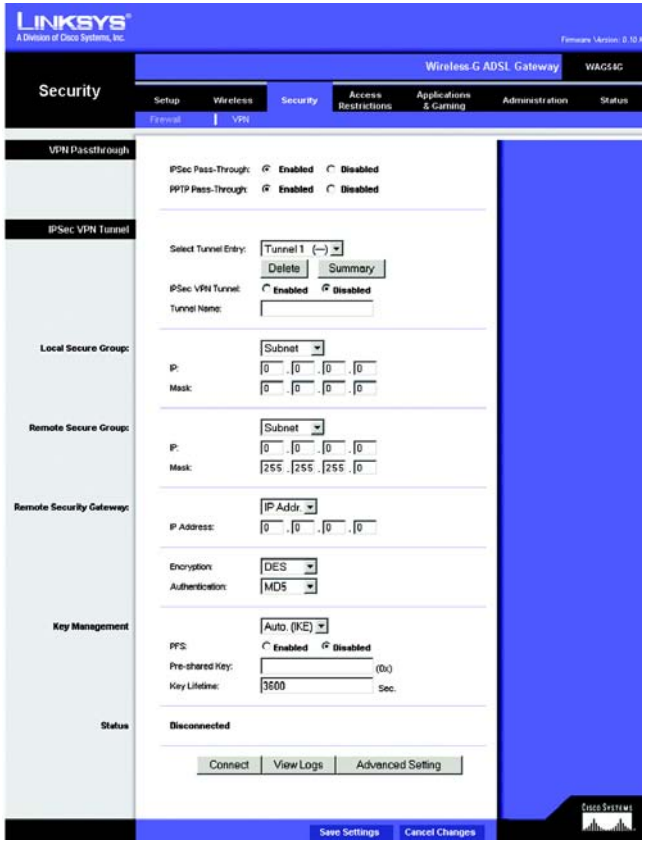

Figure C-28: VPN Tab

Appendix D: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering feature of the Gateway. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Gateway's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Gateway via a CAT 5 Ethernet network cable. See Figure D-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure D-2). This is the MAC address for your Ethernet adapter and is shown in hexadecimal as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC filtering. The example in Figure D-2 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure D-2 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

Note: The MAC address is also called the Adapter Address.

Figure D-1: IP Configuration Screen

Figure D-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.

Note: The MAC address is also called the Physical Address.

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.

3. Write down the Physical Address as shown on your computer screen (Figure D-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

   The MAC address/Physical Address is what you will use for MAC filtering. The example in Figure D-3 shows the Ethernet adapters's MAC address as 00-00-00-00-00-00. Your computer will show something different.

   The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

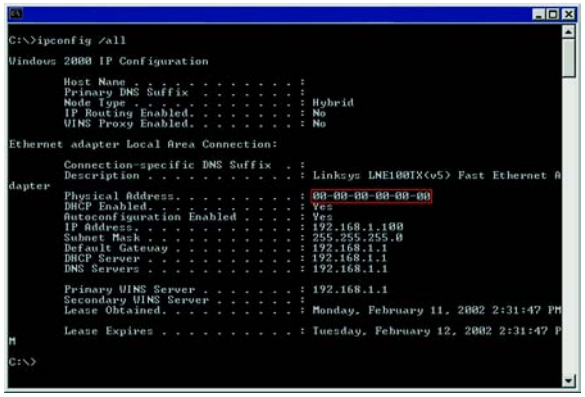
C:\>ipconfig /all
Windows 2000 IP Configuration
Host Name . . . . . :
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
Physical Address. . . . . : 00-00-00-00-00-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1
Primary WINS Server . . . . . : 192.168.1.1
Secondary WINS Server . . . . . :
Lease Obtained. . . . . : Monday, February 11, 2002 2:31:47 PM
Lease Expires . . . . . : Tuesday, February 12, 2002 2:31:47 P
M
C:\>

Figure D-3: MAC Address/Physical Address

Appendix E: Upgrading Firmware

The Gateway's firmware is upgraded through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:

1. Click the Browse button to find the firmware upgrade file that you downloaded from the Linksys international website and then extracted.

2. Double-click the firmware file you downloaded and extracted. Click the Upgrade button, and follow the instructions there.

Figure E-1: Upgrade Firmware

Appendix F: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - This is a device that adds network functionality to your computer.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a Gateway to synchronize a wireless network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Gateway's firewall protection from one computer, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (Megabits Per Second) - One million bits per second; a unit of measurement for data transmission.

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

Telnet - A user command and TCP/IP protocol used for accessing remote computers.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that uses UDP and has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix G: Specifications

Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), T1.413i2
Ports	Power, LINE (ADSL), LAN (1-4)
Buttons	One Reset Button, One On/Off Switch
Cabling Type	UTP CAT 5 or better
Data Rate	Up to 54Mbps (wireless) Up to 8Mbps downstream ADSL Up to 800kbps upstream ADSL
Transmit Power	18dBm
LEDs	Power, LAN (1-4), Wireless-G, ADSL, Act, Session
Security Features	WEP
WEP Key Bits	64, 128
Dimensions (W x H x D)	186 mm x 48 mm x 188 mm (7.32" x 1.89" x 7.40")
Unit Weight	0.48 kg (1.06 lb.)
Power	External, 12V DC, 1A
Certifications	FCC Part 15B Class B, FCC Part 15C Class B, FCC Part 68, UL 1950, CSA, CE
Operating Temp.	0ºC to 40ºC (32ºF to 104ºF)

Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix H: Regulatory Information

FCC STATEMENT

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-G ADSL Gateway conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

- EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.
- EN 609 50 Safety
- EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

- Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

- Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

- Belgique:

  Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

- France:

  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le department. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

FCC PART 68 STATEMENT

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.

SAFETY NOTICES

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this products (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

Appendix I: Warranty Information

Linksys warrants to You that, for a period of three years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

This Warranty is valid and may be processed only in the country of purchase.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix J: Contact Information

Need to contact Linksys?
Visit us online for information on the latest products and updates to your existing products at:
http://www.linksys.com/international

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Denmark	support.dk@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Portugal	support.pt@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom & Ireland	support.uk@linksys.com

Outside of Europe	E-mail Address
Latin America	support.la@linksys.com
U.S. and Canada	support@linksys.com

LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz 802.11g **Sans fil G**

WIRELESS

Passerelle ADSL **Guide de l'utilisateur**

CISCO SYSTEMS

Modèle réf. **WAG54G**

Copyright et marques commerciales

Les spécifications peuvent être modifiées sans préavis. Linksys est une marque déposée ou une marque commerciale de Cisco Systems, Inc. et/ou ses filiales aux États-Unis et dans certains autres pays. Copyright © 2004 Cisco Systems, Inc. Tous droits réservés. Les autres noms de marque et de produit sont des marques commerciales ou déposées de leurs détenteurs respectifs.

Comment utiliser ce guide ?

Ce guide présentant la Passerelle ADSL sans fil G a été conçu pour faciliter au maximum votre compréhension de la mise en réseau à l'aide de la passerelle. Les symboles suivants sont contenus dans ce Guide de l'utilisateur :

Cette coche indique un élément qui mérite une attention plus particulière lors de l'utilisation de votre passerelle.

Ce point d'exclamation indique un avertissement et vous avertit de la possibilité d'endommagement de votre installation ou de votre passerelle.

Ce point d'interrogation indique un rappel concernant quelque chose que vous êtes susceptible de devoir faire pour utiliser votre passerelle.

Outre ces symboles, les définitions concernant des termes techniques sont présentées de la façon suivante :

terme : *définition*

Chaque figure (diagramme, capture d'écran ou toute autre image) est également accompagnée d'un numéro et d'une description, comme ceci :

Figure 0-1 : Exemple de description de figure

Les numéros de figures et les descriptions sont également répertoriés à la section « Liste des figures » de la « Table des matières ».

Table des matières

Chapitre 1 : Introduction 1
Bienvenue 1
Contenu de ce guide 2
Chapitre 2 : Planification de la configuration de votre réseau 4
Les fonctions de la passerelle 4
Adresses IP 4
Qu'est ce qu'un VPN ? 5
Pourquoi ai-je besoin d'un VPN ? 6
Chapitre 3 : Présentation de la passerelle ADSL sans fil G 8
Panneau arrière 8
Panneau avant 9
Chapitre 4 : Branchement de la passerelle haut débit sans fil G 10
Présentation 10
Connexion câblée à un ordinateur 11
Connexion sans fil à un ordinateur 11
Chapitre 5 : Configuration de la passerelle 13
Présentation 13
Comment accéder à l'utilitaire Web ? 15
Onglet Setup (Configuration) 15
Onglet Wireless (Sans fil) 23
Onglet Security (Sécurité) 28
Onglet Access Restrictions (Restrictions d'accès) 33
Onglet Applications and Gaming (Applications et jeux) 35
Onglet Administration (Administration) 38
L'onglet Status (Etat) 43
Annexe A : Dépannage 47
Problèmes fréquents et solutions 47
Questions fréquemment posées 55
Annexe B : Sécurité sans fil 61
Informations importantes relatives aux périphériques sans fil 61

Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 ou Windows XP et la passerelle 64
Introduction 64
Environnement 64
Comment établir un tunnel IPSec sécurisé ? 65
Annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet 75
Instructions pour Windows 98 ou Me 75
Instructions pour Windows 2000 ou XP 76
Annexe E : Mise à niveau du micrologiciel 77
Annexe F : Glossaire 78
Annexe G : Spécifications 84
Annexe H : Réglementation 86
Annexe I : Garantie 89
Annexe J : Contacts 90

Liste des figures

Figure 2-1: Réseau 4
Figure 2-2: Passerelle connectant l'ordinateur et le réseau VPN 6
Figure 2-3: Passerelle VPN vers passerelle VPN 7
Figure 3-1: Panneau arrière 8
Figure 3-2: Panneau avant 9
Figure 4-1: Connexion Ethernet 11
Figure 4-2: Branchement du câble ADSL 11
Figure 4-3: Branchement du câble d'alimentation 11
Figure 5-1: Ecran Mot de passe 15
Figure 5-2: Onglet Basic Setup (Configuration de base) 15
Figure 5-3: Adresse IP dynamique 16
Figure 5-4: Adresse IP statique 16
Figure 5-5: RFC 1483 Routed 17
Figure 5-6: RFC 2516 PPPoE 17
Figure 5-7: RFC 2364 PPPoA 18
Figure 5-8: Bridged Mode Only 18
Figure 5-9: Optional Settings (Paramètres facultatifs) 19
Figure 5-10: DynDNS.org 20
Figure 5-11: Advanced Routing (Routage avancé) 21
Figure 5-12: Table de routage 22
Figure 5-13: Wireless Network Mode (Mode réseau sans fil). 23
Figure 5-14: WPA Pre-Shared Key (Clé WPA partagée). 24
Figure 5-15: WPA RADIUS 24
Figure 5-16: RADIUS 25
Figure 5-17: WEP 25
Figure 5-18: Wireless Network Access (Accès réseau sans fil) 26
Figure 5-19: Ordinateurs réseau 26
Figure 5-20: Advanced Wireless Settings (Paramètres sans fil avancés) 27
Figure 5-21: Firewall (Pare-feu) 28
Figure 5-22: VPN 29

Figure 5-23:	Gestion de clé manuelle	30
Figure 5-24:	Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec)	31
Figure 5-25:	Access Restriction (Restriction d'accès)	33
Figure 5-26:	Internet Policy Summary (Récapitulatif de la stratégie Internet)	33
Figure 5-27:	List of PCs (Liste des ordinateurs)	34
Figure 5-28:	Port Services (Services des ports)	34
Figure 5-29:	Single Port Forwarding (Transfert de connexion unique)	35
Figure 5-30:	Port Range Forwarding (Transfert de connexion)	36
Figure 5-31:	Port Triggering (Déclenchement de connexion)	36
Figure 5-32:	DMZ	37
Figure 5-33:	Management (Gestion)	38
Figure 5-34:	Reporting (Rapports)	40
Figure 5-35:	Ping Test (Test Ping)	41
Figure 5-36:	Factory Defaults (Paramètres d'usine)	41
Figure 5-37:	Firmware Upgrade (Mise à niveau du micrologiciel)	42
Figure 5-38:	Status (Etat)	43
Figure 5-39:	Local Network (Réseau local)	44
Figure 5-40:	Tableau des clients DHCP	44
Figure 5-41:	Wireless (Sans fil)	45
Figure 5-42:	DSL Connection (Connexion DSL)	46
Figure C-1:	Ecran Paramètres de sécurité locaux	65
Figure C-2:	Onglet Règles	65
Figure C-3:	Onglet Liste de filtres IP	65
Figure C-4:	Liste de filtres IP	66
Figure C-5:	Propriétés de Filtrer	66
Figure C-6:	Propriétés de Nouvelle règle	66
Figure C-7:	Liste de filtres IP	67
Figure C-8:	Propriétés de Filtrer	67
Figure C-9:	Propriétés de Nouvelle règle	67
Figure C-10:	Onglet Liste de filtres IP	68
Figure C-11:	Onglet Action de filtrage	68
Figure C-12:	Onglet Méthodes de sécurité	68

Figure C-13: Méthodes d'authentification 69
Figure C-14: Clé pré-partagée 69
Figure C-15: Nouvelle clé pré-partagée 69
Figure C-16: Onglet Paramètres du tunnel 70
Figure C-17: Onglet Type de connexion 70
Figure C-18: Ecran Propriétés de Nouvelle stratégie de sécurité IP 70
Figure C-19: Onglet Liste de filtres IP 71
Figure C-20: Onglet Action de filtrage 71
Figure C-21: Onglet Méthodes d'authentification 71
Figure C-22: Clé pré-partagée 72
Figure C-23: Nouvelle clé pré-partagée 72
Figure C-24: Onglet Paramètres du tunnel 72
Figure C-25: Type de connexion 73
Figure C-26: Règles 73
Figure C-27: Ordinateur local 73
Figure C-28: Onglet VPN 74
Figure D-1: Ecran de configuration IP 75
Figure D-2: Adresse MAC/Adresse de l'adaptateur 75
Figure D-3: Adresse MAC/Adresse Physique 76
Figure E-1: Mise à niveau du micrologiciel 77

Chapitre 1 : Introduction

Bienvenue

La passerelle ADSL sans fil G Linksys est la solution tout-en-un pour la connectivité Internet. La fonction modem ADSL vous offre une connexion Internet ultra-rapide, bien plus rapide que par ligne commutée et sans monopoliser votre ligne téléphonique.

Connectez votre ordinateur à la passerelle via le commutateur Ethernet 4 ports 10/100 intégré pour démarrer rapidement votre réseau. Vous pouvez partager des fichiers, des imprimantes, de l'espace disque ainsi que d'autres ressources. Branchez jusqu'à 4 ordinateurs de bureau directement ou reliez en série plusieurs concentrateurs et commutateurs pour créer un réseau dont l'extension correspond à vos besoins. Le point d'accès sans fil G intégré (802.11g) vous permet de connecter jusqu'à 32 périphériques sans fil sur votre réseau à un débit de 54 Mbit/s, sans aucun câble. Il est également compatible avec des périphériques sans fil B (802.11b), à 11 Mbit/s. La fonction routeur de la passerelle sert de « lien entre ces fonctionnalités » et permet à votre réseau de partager cette connexion Internet haut débit.

En outre, afin de protéger vos données et votre vie privée, la passerelle ADSL sans fil G dispose d'un pare-feu avancé empêchant les intrusions et les attaques par le biais d'Internet. Les transmissions sans fil peuvent être protégées par un cryptage de données puissant. La configuration est instantanée avec n'importe quel navigateur.

Avec la passerelle ADSL sans fil G Linksys au cœur de votre réseau, vous êtes en ligne avec l'avenir.

Contenu de ce guide

Ce guide de l'utilisateur présente les étapes inhérentes à l'installation et à l'utilisation de la passerelle ADSL sans fil G.

- Chapitre 1 : Introduction
  Ce chapitre présente les applications de la passerelle ADSL sans fil G ainsi que le présent Guide de l'utilisateur.

- Chapitre 2 : Planification de votre réseau
  Ce chapitre décrit les éléments de base nécessaires à la mise en place d'un réseau.

- Chapitre 3 : Présentation de la passerelle ADSL sans fil G
  Ce chapitre décrit les caractéristiques physiques de la passerelle.

- Chapitre 4 : Connexion de la passerelle ADSL sans fil G
  Ce chapitre vous explique pas à pas comment connecter la passerelle à votre réseau.

- Chapitre 5 : Configuration de la passerelle
  Ce chapitre explique comment manipuler l'utilitaire Web pour configurer les paramètres de la passerelle.

- Annexe A : Dépannage
  Cette annexe expose quelques problèmes et leurs solutions, ainsi que les questions fréquemment posées au sujet de l'installation et de l'utilisation de la passerelle ADSL sans fil G.

- Annexe B : Sécurité sans fil
  Cette annexe décrit les risques liés aux réseaux sans fil et propose quelques solutions en vue de réduire ces risques.

- Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 et la passerelle.
  Cette annexe vous explique comment établir un tunnel IPSec sécurisé à l'aide de clés partagées pour connecter un réseau privé via la passerelle VPN et une machine Windows 2000 ou XP.

- Annexe D : Mise à niveau du micrologiciel
  Cette annexe vous explique comment mettre à niveau le micrologiciel sur votre passerelle si cette opération s'avère nécessaire.

- Annexe E : Recherche des adresses MAC et IP de votre adaptateur Ethernet.
  Cette annexe explique comment rechercher l'adresse MAC de l'adaptateur Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC et/ou la fonctionnalité de clonage des adresses MAC de la passerelle.

- Annexe F : Glossaire
  Cette annexe propose un glossaire sommaire des termes fréquemment utilisés dans le cadre des réseaux.

- Annexe G : Spécifications
  Cette annexe décrit les spécifications techniques de la passerelle.

- Annexe H : Garantie
  Cette annexe fournit des informations relatives à la garantie de la passerelle.

- Annexe I : Réglementation
  Cette annexe fournit des informations relatives à la réglementation qui régit l'utilisation de la passerelle.

- Annexe J : Contacts
  Cette annexe fournit des informations sur les diverses ressources Linksys que vous pouvez contacter, notamment le Support technique.

Chapitre 2 : Planification de la configuration de votre réseau

Les fonctions de la passerelle

Une passerelle est un périphérique réseau qui connecte deux réseaux entre eux.

Dans ce cas précis, la passerelle connecte à Internet votre réseau local (LAN) ou un groupe d'ordinateurs sur votre lieu de travail ou à votre domicile. La passerelle traite et régule les données transmises entre ces deux réseaux.

La fonctionnalité NAT de la passerelle protège votre réseau d'ordinateurs, de sorte que les utilisateurs Internet publics ne puissent pas « voir » vos ordinateurs. De cette façon, votre réseau reste privé. La passerelle protège votre réseau en inspectant chaque paquet entrant via le port Internet avant qu'il soit transmis à la machine appropriée du réseau. La passerelle inspecte les services du port Internet tels que le serveur Web, le serveur FTP ou toute autre application Internet. Si elle est autorisée à le faire, elle transmet ensuite le paquet à l'ordinateur approprié du réseau local.

N'oubliez pas que les ports de la passerelle sont connectés à deux « extrémités ». Les ports LAN sont connectés à votre réseau local (LAN) et le port ADSL est connecté à Internet. Les ports LAN transmettent les données à un débit de 10/100 Mbit/s.

Figure 2-1 : Réseau

***LAN** : les ordinateurs ou produits mis en réseau qui constituent votre réseau local*

Adresses IP

Qu'est ce qu'une adresse IP ?

IP signifie Internet Protocol. Chaque périphérique d'un réseau basé sur des adresses IP, comprenant des ordinateurs, des serveurs d'impression et des passerelles, requiert une adresse IP pour l'identification de son « emplacement » ou adresse sur le réseau. Elle s'applique aux connexions LAN et Internet. Il existe deux façons d'attribuer une adresse IP à vos périphériques réseau. Vous pouvez attribuer des adresses IP statiques ou utiliser la passerelle pour attribuer dynamiquement ces adresses IP.

Adresses IP statiques

Une adresse IP statique est une adresse IP fixe que vous attribuez manuellement à un ordinateur ou à un autre périphérique du réseau. Sachant qu'une adresse IP statique reste valide jusqu'à ce que vous la désactiviez, l'utilisation d'une adresse IP statique permet de s'assurer que le périphérique correspondant aura toujours la même adresse IP tant que vous ne la changez pas. Les adresses IP statiques doivent être uniques et sont généralement utilisées avec des périphériques réseau tels que les serveurs d'ordinateurs ou les serveurs d'impression.

REMARQUE : Etant donné que la passerelle est un périphérique connecté à deux réseaux, elle requiert deux adresses IP : une pour le LAN et une pour Internet. Dans ce Guide de l'utilisateur, vous trouverez des références à l'« adresse IP Internet » et à l'« adresse IP LAN ».

Puisque la passerelle utilise la technologie NAT, la seule adresse IP de votre réseau qui peut être « vue » à partir d'Internet est l'adresse IP Internet de la passerelle. Néanmoins, même cette adresse IP peut être bloquée, pour que la passerelle et le réseau soient invisibles sur Internet. Veuillez vous reporter à la section décrivant les requêtes WAN de la rubrique Sécurité du « Chapitre 5 : Configuration de la passerelle ».

Etant donné que vous utilisez la passerelle pour partager votre connexion Internet DSL, contactez votre fournisseur d'accès Internet pour savoir si une adresse IP statique a été attribuée à votre compte. Si c'est le cas, vous aurez besoin de cette adresse IP statique lors de la configuration de votre passerelle. Vous pouvez obtenir cette information en contactant votre fournisseur d'accès Internet (FAI).

Adresses IP dynamiques

Une adresse IP dynamique est automatiquement attribuée à un périphérique du réseau, tel qu'un ordinateur ou un serveur d'impression. Ces adresses IP sont dites « dynamiques » car elles sont attribuées temporairement à l'ordinateur ou au périphérique. A l'issue d'un délai déterminé, elles expirent et sont remplacées. Si un ordinateur se connecte au réseau (ou à Internet) et que son adresse IP dynamique a expiré, le serveur DHCP lui attribue automatiquement une nouvelle adresse IP dynamique.

Serveurs DHCP (Dynamic Host Configuration Protocol)

Les ordinateurs et tous les autres périphériques réseau utilisant des adresses IP dynamiques se voient attribuer une nouvelle adresse IP par un serveur DHCP. L'ordinateur ou le périphérique réseau qui obtient une adresse IP est appelé le client DHCP. DHCP vous évite d'avoir à attribuer des adresses IP manuellement dès qu'un nouvel utilisateur est ajouté à votre réseau.

Un serveur DHCP peut être soit un ordinateur dédié du réseau, soit un autre périphérique réseau, tel que la passerelle. Par défaut, la fonction de serveur DHCP de la passerelle est activée.

Si vous disposez déjà d'un serveur DHCP sur votre réseau, vous devez désactiver l'un des deux serveurs DHCP. Si vous exécutez plusieurs serveurs DHCP sur votre réseau, des erreurs se produisent, telles que des conflits d'adresses IP. Pour désactiver la fonction DHCP sur la passerelle, reportez-vous à la rubrique relative au DHCP du « Chapitre 5 : Configuration de la passerelle ».

Qu'est ce qu'un VPN ?

Un VPN (Virtual Private Network - réseau privé virtuel) est une connexion (une passerelle VPN, par exemple) entre deux points terminaux de différents réseaux, qui permet la transmission de données privées sur un réseau partagé ou public, tel que l'Internet. Cette structure permet la transmission sécurisée de données d'un réseau privé entre ces deux emplacements ou réseaux.

Cette opération nécessite la création d'un « tunnel ». Un tunnel VPN connecte deux ordinateurs ou réseaux et permet aux données d'être transmises via Internet comme si elles étaient toujours sur ces réseaux. Il ne s'agit évidemment pas d'un tunnel mais d'une connexion sécurisée grâce au cryptage des données transmises entre les deux réseaux.

Le VPN (réseau privé virtuel) est une solution offrant un excellent rapport coût/efficacité, qui se substitue à la ligne louée, privée et dédiée d'un réseau privé. Grâce à l'utilisation des techniques standard de l'industrie en matière de cryptage et d'authentification, appelées IPSec (abréviation de IP Security), le VPN crée une connexion sécurisée qui fonctionne effectivement comme si vous étiez directement connecté à votre réseau local. Le VPN peut être utilisé pour créer des liaisons réseau sécurisées entre le siège d'une entreprise et ses filiales. Il est également destiné au télé-travail et/ou aux professionnels souvent en déplacement. Ces derniers peuvent se connecter à une passerelle VPN à partir de n'importe quel ordinateur sur lequel un logiciel client VPN prenant en charge IPSec est installé (SSH Sentinel, par exemple.)

Il existe deux façons très simples de créer une connexion VPN :

- Passerelle VPN vers passerelle VPN
- Ordinateur (utilisant le logiciel client VPN qui prend en charge IPSec) vers passerelle VPN

La passerelle VPN crée un tunnel ou canal entre les deux points terminaux. Ainsi les données transitant entre ces deux points terminaux sont sécurisées. Un ordinateur équipé d'un logiciel client VPN prenant en charge IPSec peut être l'un des deux points terminaux. Tout ordinateur équipé du IPSec Security Manager (Microsoft 2000 et XP) intégré permet à la passerelle VPN de créer un tunnel VPN à l'aide de IPSec. Reportez-vous à l'« Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 ou XP et la passerelle VPN ». D'autres versions de systèmes d'exploitation Microsoft requièrent l'installation de logiciels client VPN tiers supplémentaires qui prennent en charge IPSec.

Ordinateur (utilisant le logiciel client VPN qui prend en charge IPSec) vers passerelle VPN

Voici un exemple d'installation VPN entre un ordinateur et une passerelle VPN. (figure 2-2) Dans sa chambre d'hôtel, une femme en déplacement pour son travail se connecte à son fournisseur d'accès Internet. Sur son ordinateur portable, le logiciel client VPN est configuré avec les paramètres VPN de son bureau. Elle accède au logiciel client VPN qui prend en charge IPSec et se connecte à la passerelle VPN au siège de sa société. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. Grâce au VPN, cette personne dispose maintenant d'une connexion sécurisée au réseau du siège de sa société, comme si elle y était physiquement connectée.

Passerelle VPN vers passerelle VPN

Voici un exemple d'installation VPN entre deux passerelles VPN. (figure 2-3) A son domicile, un télé-travailleur utilise sa passerelle VPN pour sa connexion Internet continue. Sa passerelle est configurée avec les paramètres VPN de son bureau. Lorsqu'il se connecte à la passerelle de son bureau, les deux passerelles créent un tunnel VPN, permettant le cryptage et le décryptage des données. Puisque les VPN utilisent Internet, la distance ne pose aucun problème. A l'aide du VPN, le télé-travailleur dispose ainsi d'une connexion sécurisée au réseau du siège de sa société, comme s'il y était physiquement connecté.

Pour obtenir de plus amples informations et des instructions sur la création de votre propre VPN, veuillez consulter le site Web international de Linksys à www.linksys.com/international ou reportez-vous à l'« Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 ou XP et la passerelle VPN ».

Pourquoi ai-je besoin d'un VPN ?

La mise en réseau d'ordinateurs offre une flexibilité que l'on ne trouve pas sur un système classique d'échange de données (documents papiers). Cette flexibilité s'accompagne néanmoins d'un risque plus important en matière de sécurité. C'est pour cette raison que les pare-feu ont été mis en place. Les pare-feu aident à protéger les données d'un réseau local. Cependant, que faites-vous une fois que les informations sont envoyées hors de votre réseau local, lorsque des messages électroniques sont envoyés à leur destinataire ou lorsque vous êtes en déplacement et que vous devez vous connecter au réseau de votre société ? Comment vos données sont-elles protégées ?

Ordinateur portable utilisant le logiciel client VPN qui prend en charge IPSec
INTERNET
A distance
Routeur VPN au siège de la société

Figure 2-2 : Passerelle connectant l'ordinateur et le réseau VPN

IMPORTANT : Vous devez installer au moins une passerelle VPN à une extrémité du tunnel VPN. A l'autre extrémité du tunnel VPN, vous devez installer une seconde passerelle VPN ou un ordinateur équipé du logiciel client VPN prenant en charge IPSec.

Le VPN est la solution à vos problèmes. Les VPN sécurisent les données transmises à l'extérieur de votre réseau comme si elles étaient toujours sur votre réseau.

Lorsque des données sont envoyées à l'extérieur via Internet à partir de votre ordinateur, elles sont toujours vulnérables. Il se peut que vous ayez déjà un pare-feu, qui vous aide à protéger les données transmises sur votre réseau ou contenues sur ce dernier contre des corruptions ou interceptions par des entités extérieures. Néanmoins, dès que ces données quittent votre réseau, lorsque vous envoyez des données par message électronique ou que vous communiquez via Internet, le pare-feu ne les protège plus.

A ce stade, vos données deviennent alors accessibles aux pirates qui utilisent diverses méthodes pour voler non seulement les données que vous transmettez mais aussi vos informations de connexion réseau et de sécurité. Les méthodes les plus couramment utilisées sont décrites ci-après :

1) Usurpation d'adresses MAC (MAC Address Spoofing)

Les paquets transmis sur un réseau, soit votre réseau local, soit Internet, sont précédés d'un en-tête de paquet. Ces en-têtes de paquet contiennent les informations de source et de destination permettant au paquet d'être transmis efficacement. Un pirate peut utiliser ces informations pour usurper l'adresse MAC autorisée sur un réseau. Avec cette adresse MAC usurpée, le pirate peut également intercepter des informations destinées à un autre utilisateur.

2) Analyse des données (Data Sniffing)

L'analyse des données est une méthode utilisée par les pirates pour obtenir des données réseau transmises sur des réseaux non-sécurisés tels que Internet. Les outils permettant ce type d'activité, tels que les analyseurs de protocole et les outils de diagnostic réseau, sont souvent intégrés aux systèmes d'exploitation et les données peuvent être visualisées normalement.

3) Attaques centralisées (Man in the Middle Attacks)

Une fois que le pirate a analysé ou usurpé suffisamment d'informations, il peut entreprendre une attaque centralisée. Cette attaque est réalisée lorsque les données sont transmises d'un ordinateur à un autre, en déroutant les données vers une autre destination. Même si les données ne sont pas reçues par le destinataire d'origine, l'expéditeur ne le sait pas.

Il s'agit seulement d'une petite partie des méthodes utilisées par les pirates qui ne cessent de perfectionner leurs techniques. Sans la sécurité d'un VPN, vos données sont constamment à la merci de telles attaques lorsqu'elles sont transmises via Internet. Les données transmises via Internet transitent souvent par de nombreux serveurs dans le monde avant d'arriver à destination. Ce parcours est très long lorsqu'il s'agit de données non-sécurisées, ce qui montre bien tout l'intérêt du VPN.

Figure 2-3 : Passerelle VPN vers passerelle VPN

Chapitre 3 : Présentation de la passerelle ADSL sans fil G

Panneau arrière

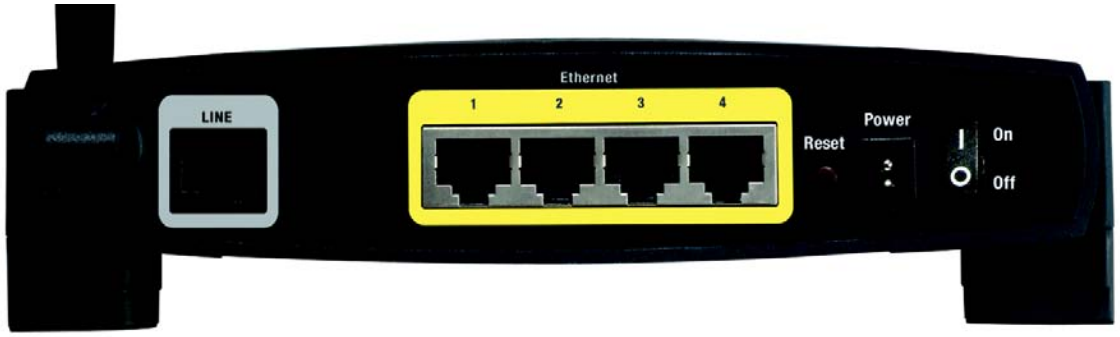

Figure 3-1 : Panneau arrière

Les ports de la passerelle permettant notamment de connecter le câble réseau, sont situés sur le panneau arrière de l'appareil. Les boutons de la passerelle sont également situés sur le panneau arrière de l'appareil.

LINE Le port **LINE (LIGNE)** permet de connecter la câble ADSL.

Ethernet (1-4) Les ports **Ethernet** (Ethernet) permettent de connecter l'appareil à votre ordinateur et à d'autres périphériques réseau.

Power Le port **Power** (Alimentation) permet de connecter l'adaptateur électrique.

Bouton Reset Il existe deux façons de réinitialiser les paramètres d'usine de votre passerelle : soit en appuyant sur le **bouton Reset** (Réinitialiser) pendant une dizaine de secondes, soit en accédant à l'écran Factory Defaults (Paramètres d'usine) dans l'onglet Administration (Administration) de l'utilitaire Web de la passerelle.

On/Off Ce commutateur permet d'allumer ou d'éteindre la passerelle.

Grâce à ces fonctions, et à bien d'autres produits Linksys, vos options de gestion de réseau sont illimitées. Pour obtenir de plus amples informations sur les produits compatibles avec la passerelle, consultez le site Web international de Linksys à www.linksys.com/international.

Important : La réinitialisation des paramètres d'usine de la passerelle supprime tous les paramètres personnalisés (Cryptage WEP, paramètres de connexion sans fil et LAN, etc.). Ne réinitialisez pas les paramètres de la passerelle si vous souhaitez les conserver.

Panneau avant

Les voyants de la passerelle, qui vous informent de l'activité du réseau, se trouvent sur le panneau avant.

Figure 3-2 : Panneau avant

Alimentation Vert. Le voyant **Power** (Alimentation) s'allume lorsque l'adaptateur est sous tension.

Ethernet (1-4) Vert. Le voyant **LAN** (LAN) a deux fonctions. S'il est allumé en permanence, cela signifie que la passerelle est connectée correctement à un périphérique via le port LAN (réseau local). S'il clignote, il indique une activité réseau.

WLAN Vert. Le voyant **WLAN** s'allume lorsqu'une connexion sans fil est réalisée avec succès. S'il clignote, cela signifie que la passerelle envoie des données à l'un des périphériques du réseau ou reçoit des données de l'un des périphériques du réseau.

DSL Vert. Le voyant **DSL** s'allume lorsqu'une connexion DSL est réalisée avec succès. Il clignote au moment de l'établissement de la connexion.

Internet Vert. Le **voyant Internet** est vert lorsqu'une connexion au fournisseur d'accès Internet (FAI) a été établie. Le voyant **Internet** est rouge si la connexion au fournisseur d'accès Internet (FAI) a échoué.

Chapitre 4 : Branchement de la passerelle haut débit sans fil G

Présentation

La configuration de la passerelle ne consiste pas seulement à connecter les appareils entre eux. Vous devez configurer vos ordinateurs du réseau pour qu'ils acceptent les adresses IP que leur attribue la passerelle (le cas échéant). Vous devez également configurer la passerelle à l'aide des paramètres fournis par votre fournisseur d'accès Internet (FAI).

Le technicien de votre fournisseur d'accès Internet doit vous avoir communiqué les données concernant votre modem après avoir installé votre connexion haut débit. Si ce n'est pas le cas, contactez votre FAI.

Si vous disposez des informations de configuration correspondant à votre type de connexion Internet, vous pouvez commencer l'installation et la configuration de votre passerelle.

Si vous souhaitez utiliser un ordinateur équipé d'un adaptateur Ethernet pour configurer la passerelle, passez à la rubrique « Connexion câblée à un ordinateur ». Si vous souhaitez utiliser un ordinateur équipé d'un adaptateur sans fil pour configurer la passerelle, passez à la rubrique « Connexion sans fil à un ordinateur ».

Connexion câblée à un ordinateur

1. Avant de commencer, vérifiez que tous les appareils du réseau sont hors tension, y compris la passerelle et tous les ordinateurs.
2. Reliez une extrémité d'un câble réseau Ethernet à l'un des ports Ethernet (numérotés de 1 à 4) situés sur le panneau arrière de la passerelle (figure 4-1) et l'autre extrémité au port Ethernet d'un ordinateur.
3. Procédez de même pour relier d'autres ordinateurs, un commutateur ou des périphériques réseau à la passerelle.

IMPORTANT : Si vous utilisez des microfiltres, placez-les uniquement entre le téléphone et la prise murale et non pas entre la passerelle et la prise murale sinon votre connexion ADSL ne sera pas établie.

4. Branchez un câble téléphonique entre le port Line (Ligne) du panneau arrière de la passerelle (figure 4-2) et la prise murale de ligne ADSL. Les utilisateurs Annex A doivent placer un microfiltre entre chaque téléphone et prise murale afin d'éliminer les interférences. Les utilisateurs Annex B (ADSL via RNIS) doivent utiliser des séparateurs si nécessaire. Pour plus d'informations, veuillez contacter votre FAI.
5. Branchez l'adaptateur électrique au port Power (Alimentation) de la passerelle (figure 4-3) puis raccordez l'autre extrémité à une prise d'alimentation électrique. Appuyez sur le bouton On/Off (Marche/Arrêt).
   - Le voyant Power (Alimentation) situé sur le panneau avant est vert dès que l'adaptateur électrique est correctement connecté et que le bouton est en position On (Marche). Le voyant Power (Alimentation) clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».
6. Allumez un des ordinateurs connectés à la passerelle.

Figure 4-1 : Connexion Ethernet

Figure 4-2 : Branchement du câble ADSL

REMARQUE : Branchez toujours l'adaptateur électrique de la passerelle sur une barrette de connexion protégée contre les surtensions.

Connexion sans fil à un ordinateur

Si vous souhaitez utiliser une connexion sans fil pour accéder à la passerelle, procédez comme suit :

1. Avant de commencer, vérifiez que tous les appareils du réseau sont hors tension, y compris la passerelle et tous les ordinateurs.

Figure 4-3 : Branchement du câble d'alimentation

IMPORTANT : Si vous utilisez des microfiltres, placez-les uniquement entre le téléphone et la prise murale et non pas entre la passerelle et la prise murale sinon votre connexion ADSL ne sera pas établie.

2. Branchez un câble téléphonique entre le port Line (Ligne) du panneau arrière de la passerelle (figure 4-2) et la prise murale de ligne ADSL. Il peut être nécessaire de placer un microfiltre entre chaque téléphone et prise murale pour éliminer les interférences. Pour plus d'informations, veuillez contacter votre FAI.

3. Connectez l'adaptateur électrique fourni au port Power (Alimentation) (figure 4-3) puis branchez-le sur une prise d'alimentation. Appuyez sur le bouton On/Off (Marche/Arrêt).

   - Le voyant Power (Alimentation) situé sur le panneau avant est vert dès que l'adaptateur électrique est correctement connecté et que le bouton est en position On (Marche). Le voyant d'alimentation clignote pendant quelques secondes puis reste allumé une fois le test d'autodiagnostic terminé. Si le voyant clignote pendant au moins une minute, reportez-vous à l'« Annexe A : Dépannage ».

4. Allumez un des ordinateurs de votre/vos réseau(x) sans fil.

5. Pour accéder initialement à la passerelle via une connexion sans fil, assurez-vous que le SSID de l'adaptateur sans fil est défini à « linksys » (paramètre par défaut de la passerelle) et que son cryptage WEP est désactivé. Après avoir accédé à la passerelle, vous pouvez modifier les paramètres de la passerelle et de l'adaptateur de cet ordinateur pour qu'ils correspondent à vos paramètres réseau standard.

REMARQUE : Veillez à toujours modifier les paramètres par défaut SSID Linksys et activer le cryptage WEP.

L'installation matérielle de la passerelle est maintenant terminée.

Vous pouvez dès à présent passer au « Chapitre 5 : Configuration de la passerelle ».

Chapitre 5 : Configuration de la passerelle

Présentation

Suivez les étapes contenues dans ce chapitre et utilisez l'utilitaire Web de la passerelle pour configurer cette dernière. Ce chapitre décrit chaque page Web de l'utilitaire ainsi que les fonctions clés de chaque page. Vous pouvez accéder à l'utilitaire à partir de votre navigateur Web par l'intermédiaire d'un ordinateur connecté à la passerelle. Dans le cadre d'une configuration réseau de base, la plupart des utilisateurs pourront effectuer leurs opérations uniquement à partir des écrans de l'utilitaire suivants :

- Basic Setup (Configuration de base). Dans l'écran Basic Setup (Configuration de base), entrez les paramètres fournis par votre fournisseur d'accès Internet (FAI).
- Management (Gestion). Cliquez sur l'onglet **Administration** (Administration) puis sur l'onglet **Management** (Gestion). Le nom d'utilisateur et le mot de passe par défaut de la passerelle est admin. Pour sécuriser la passerelle, choisissez un mot de passe autre que le mot de passe par défaut.

Sept onglets principaux sont disponibles : Setup (Configuration), Wireless (Sans fil), Security (Sécurité), Access Restrictions (Restrictions d'accès), Applications & Gaming (Applications et jeux), Administration (Administration) et Status (Etat). D'autres onglets apparaissent dès que vous cliquez sur l'un des onglets principaux.

Setup (Configuration)

- Basic Setup (Configuration de base). Entrez les paramètres de connexion Internet et de réseau dans cet écran.
- DDNS. Pour activer la fonctionnalité DDNS (Dynamic Domain Name System) de la passerelle, renseignez les champs à l'écran.
- Advanced Routing (Routage avancé). Dans cet écran, vous pouvez configurer les options de Dynamic Routing (Routage dynamique) et Static Routing (Routage statique).

Wireless (Sans fil)

- Basic Wireless Settings (Paramètres sans fil de base). Dans cet écran, vous pouvez sélectionner les options Wireless Network Mode (Mode de réseau sans fil) et Wireless Security (Sécurité sans fil).
- Wireless Network Access (Accès réseau sans fil). Cet écran contient votre liste d'accès au réseau sans fil.
- Advanced Wireless Settings (Paramètres sans fil avancés). Dans cet écran, vous pouvez accéder aux fonctionnalités Advanced Wireless Settings (Paramètres sans fil avancés).

Security (Sécurité)

- Firewall (Pare feu). Cet écran permet de définir les options Filters (Filtres) et Block Wan Requests (Blocage des requêtes WAN). Les filtres permettent d'empêcher des utilisateurs internes d'accéder à Internet mais aussi de bloquer les requêtes Internet anonymes.

Avez-vous activé TCP/IP sur vos ordinateurs ? Les ordinateurs utilisent ce protocole pour communiquer sur le réseau. Pour obtenir plus d'informations sur TCP/IP, reportez-vous à l'Annexe D (Aide Windows).

Remarque : Pour plus de sécurité, modifiez votre mot de passe à partir de l'onglet Administration (Administration).

- VPN. Cet écran permet d'activer ou de désactiver IPSec et/ou l'intercommunication PPTP mais aussi de configurer des tunnels VPN.

Access Restrictions (Restrictions d'accès)

- Internet Access (Accès Internet). Cet écran permet d'autoriser ou non l'accès au réseau aux utilisateurs souhaités.

Applications & Gaming (Applications et jeux)

- Single Port Forwarding (Transfert de connexion unique). Cet écran vous permet de configurer des services ou des applications standard sur votre réseau.
- Port Range Forwarding (Transfert de connexion). Cet onglet vous permet de configurer des services publics ou d'autres applications Internet spécialisées sur votre réseau.
- Port Triggering (Déclenchement de connexion). Cet onglet vous permet de configurer des connexions déclenchées et des connexions transférées pour des applications Internet.
- DMZ. Cet écran vous permet d'autoriser l'exposition à Internet d'un utilisateur local, pour l'accès à des services spécifiques.

Administration (Administration)

- Management (Gestion). Dans cet écran, vous pouvez définir vos privilèges d'accès à la passerelle ainsi que vos paramètres SNMP et UPnP.
- Reporting (Rapports). Cet onglet vous permet de visualiser ou d'enregistrer des fichiers journaux d'activités.
- Diagnostics (Diagnostics). Cet écran vous permet d'effectuer un test Ping.
- Factory Defaults (Paramètres d'usine). Cet écran vous permet de restaurer les paramètres d'usine (par défaut) de la passerelle.
- Firmware Upgrade (Mise à niveau du micrologiciel). Cet onglet vous permet de mettre à niveau le micrologiciel de la passerelle.

Status (Etat)

- Gateway (Passerelle). Cet écran contient des informations sur l'état de la passerelle.
- Local Network (Réseau local). Cet écran contient des informations sur l'état du réseau local.
- Wireless (Sans fil). Cet écran contient des informations sur l'état du réseau sans fil.
- DSL Connection (Connexion DSL). Cet écran contient des informations sur l'état de la connexion DSL.

Comment accéder à l'utilitaire Web ?

Pour accéder à l'utilitaire Web, démarrez Internet Explorer ou Netscape Navigator, puis entrez l'adresse IP par défaut de la passerelle (192.168.1.1) dans le champ Adresse. Appuyez ensuite sur la touche Entrée.

Une page demandant la saisie d'un mot de passe apparaît (figure 5-1). (écran similaire pour les utilisateurs de systèmes autres que Windows XP) Entrez **admin** (nom d'utilisateur par défaut) dans le champ User Name (Nom d'utilisateur) et **admin** (mot de passe par défaut) dans le champ Password (Mot de passe). Cliquez sur le bouton **OK**.

Mot de passe réseau
Entrez votre nom d'utilisateur et votre mot de passe.
Site/pare-feu : 192.168.1.1
Domaine Linksys WAG54G
Nom de l'utilisateur admin
Mot de passe
Enregistrer ce mot de passe dans votre liste de mots de passe
OK
Annuler

Figure 5-1 : Ecran Mot de passe

Onglet Setup (Configuration)

Onglet Basic Setup (Configuration de base)

Le premier écran qui s'affiche est l'onglet Basic Setup (Configuration de base). (figure 5-2.) Cet onglet vous permet de modifier les paramètres généraux de la passerelle. Modifiez ces paramètres comme décrit ci-contre, puis cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-2 : Onglet Basic Setup (Configuration de base)

Internet Setup (Configuration Internet)

- VC Settings (Paramètres VC). Virtual Circuit (Circuit Virtuel) : ces champs (VPI et VCI) se rapportent à deux éléments : VPI (Virtual Path Identifier) et VCI (Virtual Channel Identifier). Votre FAI vous indiquera le paramétrage approprié de chacun de ces deux champs. Multiplexing (Multiplexage) : sélectionnez **LLC** ou **VC** en fonction de votre FAI.
- ADSL Settings (Paramètres ADSL). La passerelle prend en charge cinq encapsulations : RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA et Bridged Mode Only. Les écrans Basic Setup (Configuration de base) et les options disponibles varient selon le type d'encapsulation sélectionné.

RFC 1483 Bridged

Adresse IP dynamique

IP Settings (Paramètres IP). Sélectionnez **Obtain an IP Address Automatically** (Obtenir une adresse IP automatiquement) si votre FAI vous indique que vous êtes connecté via une adresse IP dynamique. (figure 5-3)

Adresse IP statique

Si vous devez utiliser une adresse IP permanente pour vous connecter à Internet, sélectionnez **Use the following IP Address** (Utiliser l'adresse IP suivante). (figure 5-4)

- IP Address (Adresse IP). Il s'agit de l'adresse IP de la passerelle, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau de la passerelle. Votre FAI peut vous fournir le masque de sous-réseau.
- Default Gateway (Passerelle par défaut). Votre FAI peut vous fournir l'adresse par défaut de la passerelle. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine principal). Il est obligatoire. Secondary DNS (Nom de domaine secondaire). Il est facultatif. Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

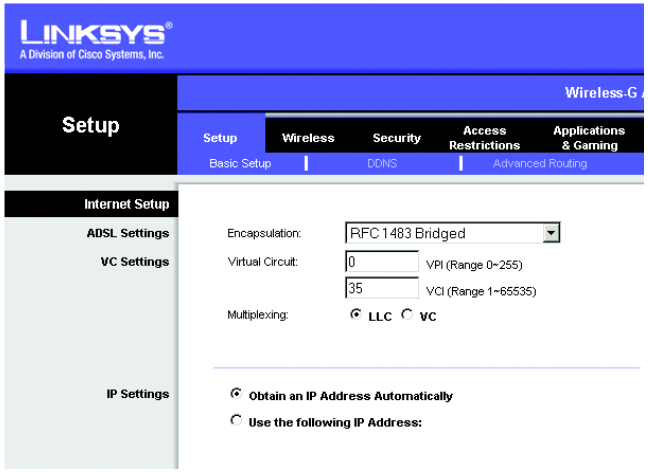

Figure 5-3 : Adresse IP dynamique

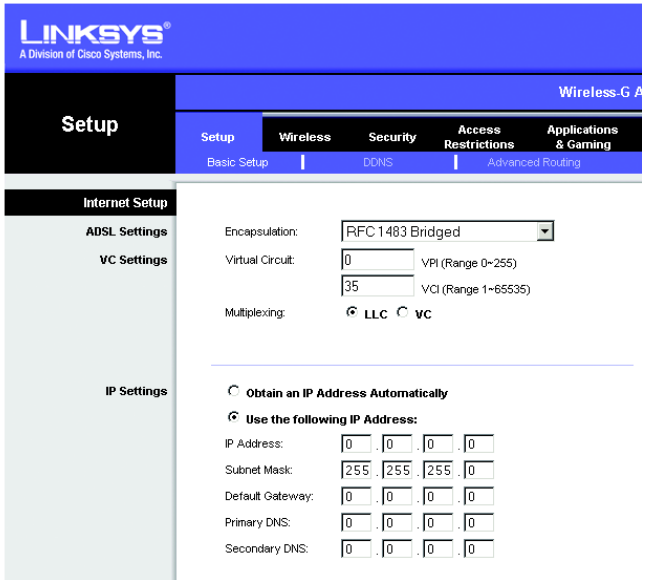

Figure 5-4 : Adresse IP statique

RFC 1483 Routed

Si vous devez utiliser RFC 1483 Routed, sélectionnez **RFC 1483 Routed**. (figure 5-5)

- IP Address (Adresse IP). Il s'agit de l'adresse IP de la passerelle, vue par le WAN ou Internet. Votre FAI peut vous fournir l'adresse IP que vous devez spécifier dans ce champ.
- Subnet Mask (Masque de sous-réseau). Il s'agit du masque de sous-réseau de la passerelle. Votre FAI peut vous fournir le masque de sous-réseau.
- Default Gateway (Passerelle par défaut). Votre FAI peut vous fournir l'adresse par défaut de la passerelle. Il s'agit en fait de l'adresse IP du serveur du FAI.
- Primary DNS (Nom de domaine principal). Il est obligatoire. Secondary DNS (Nom de domaine secondaire). Il est facultatif. Votre FAI peut vous fournir au moins une adresse IP de serveur DNS (Domain Name System).

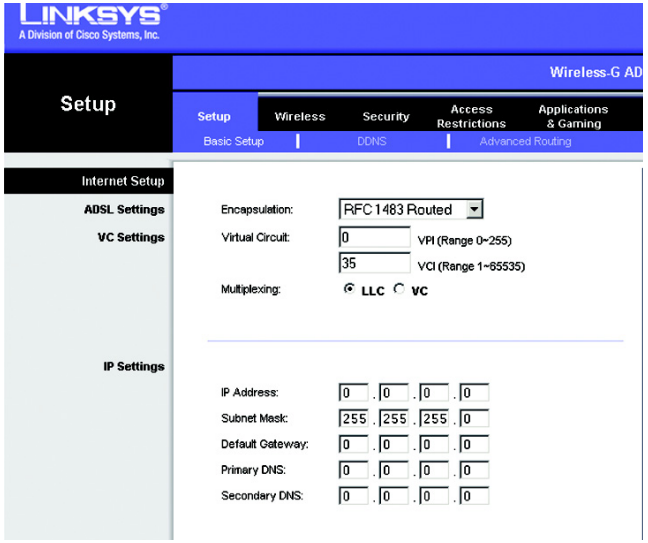

Figure 5-5 : RFC 1483 Routed

RFC 2516 PPPoE

Certains fournisseurs d'accès Internet (FAI) DSL utilisent le protocole PPPoE (protocole de point-à-point sur Ethernet) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoE. Si tel est le cas, vous devrez sélectionner l'option PPPoE. (figure 5-6)

- Service Name (Nom du service). Entrez le nom du service, s'il est requis par votre FAI.
- User Name (Nom d'utilisateur) et Password (Mot de passe). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand: Max Idle Time (Connexion à la demande : délai d'inactivité maximal). Vous pouvez configurer la passerelle afin qu'elle désactive la connexion Internet après une période donnée d'inactivité (Max Idle Time). Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet à la passerelle de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Connect on Demand** (Connexion à la demande). Dans le champ Max Idle Time (Délai d'inactivité maximal), entrez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Keep Alive: Redial Period (Activée : rappel après). Si vous sélectionnez cette option, la passerelle procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, la passerelle rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive** (Activée). Dans le champ Redial Period (rappel après), spécifiez la fréquence à laquelle la passerelle doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de 30 secondes.

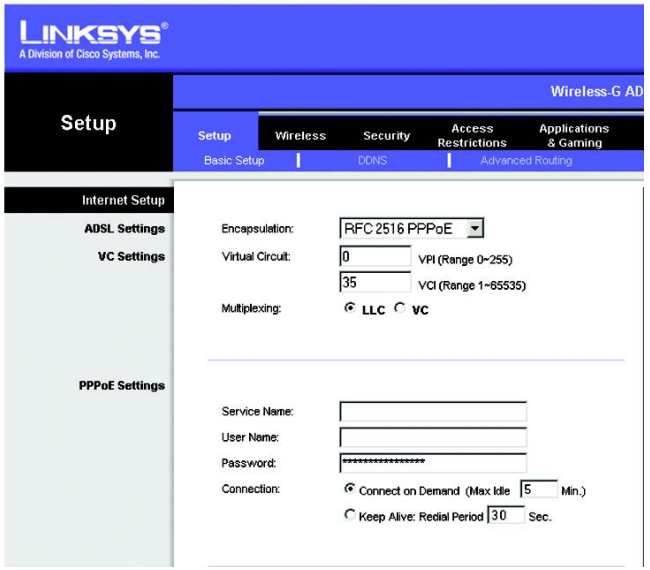

Figure 5-6 : RFC 2516 PPPoE

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

RFC 2364 PPPoA

Certains fournisseurs d'accès Internet (FAI) DSL utilisent le protocole PPPoA (protocole de point-à-point sur ATM) pour établir des connexions Internet. Si vous êtes connecté à Internet par l'intermédiaire d'une ligne DSL, demandez à votre FAI s'il utilise le protocole PPPoA. Si tel est le cas, vous devrez sélectionner l'option PPPoA. (figure 5-7)

- User Name (Nom d'utilisateur) et Password (Mot de passe). Entrez le nom d'utilisateur et le mot de passe fournis par votre FAI.
- Connect on Demand: Max Idle Time (Connexion à la demande : délai d'inactivité maximal). Vous pouvez configurer la passerelle afin qu'elle désactive la connexion Internet après une période donnée d'inactivité (Max Idle Time). Si votre connexion Internet a été désactivée suite à son inactivité, l'option Connect on Demand (Connexion à la demande) permet à la passerelle de rétablir automatiquement votre connexion dès que vous tentez d'accéder de nouveau à Internet. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Connect on Demand** (Connexion à la demande). Dans le champ Max Idle Time (Délai d'inactivité maximal), entrez le nombre de minutes que vous souhaitez voir s'écouler avant la désactivation de votre connexion Internet.
- Keep Alive: Redial Period (Activée : rappel après). Si vous sélectionnez cette option, la passerelle procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, la passerelle rétablit automatiquement votre connexion. Si vous souhaitez sélectionner cette option, cliquez sur le bouton radio **Keep Alive** (Activée). Dans le champ Redial Period (rappel après), spécifiez la fréquence à laquelle la passerelle doit vérifier votre connexion Internet. Le temps devant s'écouler par défaut avant rappel est de 30 secondes.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

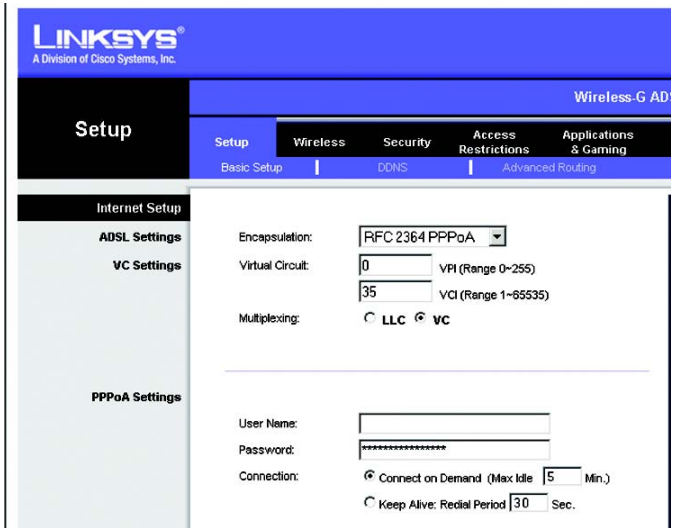

Figure 5-7 : RFC 2364 PPPoA

Bridged Mode Only

Si vous utilisez votre passerelle en tant que pont (elle fonctionne comme un modem autonome, sélectionnez **Bridged Mode Only**. (figure 5-8) La technologie NAT et le routage sont désactivés dans ce mode.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

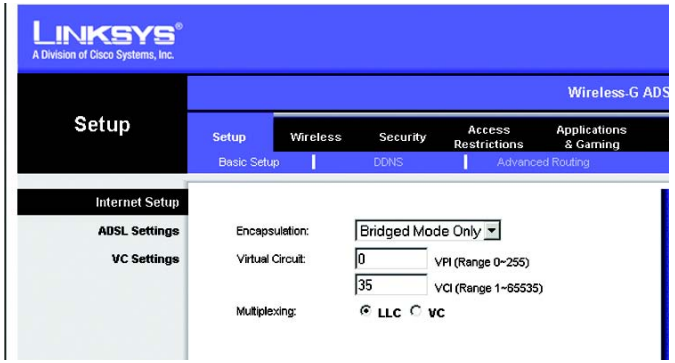

Figure 5-8 : Bridged Mode Only

Optional Settings (Required by some ISPs) (Paramètres facultatifs) (requis par certains FAI) (figure 5-9).

- Host Name/Domain Name (Nom d'hôte/Nom de domaine). Entrez les noms d'hôte et de domaine de la passerelle dans ces deux champs. Certains FAI requièrent ces noms pour l'authentification. Il se peut que vous deviez contacter votre FAI pour vérifier si votre service Internet haut débit a été configuré avec un nom d'hôte et un nom de domaine. Dans la plupart des cas, vous pourrez laisser ces champs vides.

- MTU. Le paramètre MTU (Maximum Transmission Unit) spécifie la taille de paquet maximale autorisée pour la transmission réseau. Sélectionnez **Manual** (Manuel) et entrez la valeur souhaitée. Il est recommandé d'entrer une valeur comprise entre 1200 et 1500. Par défaut, le paramètre MTU est configuré automatiquement.

Network Setup (Configuration réseau)

- Router IP (Adresse IP du routeur). Les valeurs d'adresse IP locale et de masque de sous-réseau de la passerelle sont spécifiées dans ces champs. Dans la plupart des cas, il est recommandé de conserver les valeurs par défaut.
  - Local IP Address (Adresse IP locale). La valeur par défaut est 192.168.1.1.
  - Subnet Mask (Masque de sous-réseau). La valeur par défaut est 255.255.255.0.
- Network Address Server Settings (DHCP) (Paramètres du serveur d'adresse de réseau DHCP) Un serveur Dynamic Host Configuration Protocol (DHCP) attribue automatiquement une adresse IP à chaque ordinateur du réseau. A moins que vous ne disposiez déjà d'un serveur DHCP, il est recommandé de laisser la fonction de serveur DHCP activée pour la passerelle.
  - Local DHCP Server (Serveur DHCP local). Cette option est activée par défaut. Si vous disposez déjà d'un serveur DHCP sur votre réseau, sélectionnez **Disable** (Désactiver). Relais DHCP
  - Starting IP Address (Adresse IP de départ). Entrez une valeur de départ pour la publication d'adresses IP sur le serveur DHCP. Cette valeur doit être 192.168.1.2 ou supérieure, car l'adresse IP par défaut de la passerelle est 192.168.1.1.
  - Number of Address (Nombre d'adresses). Entrez le nombre maximal d'ordinateurs auquel le serveur DHCP doit attribuer des adresses IP. Ce nombre ne peut pas être supérieur à 253. Par défaut (figure 5-9), elle est comprise entre 192.168.1.100 et 192.168.1.149.
  - DHCP Address Range (Etendue des adresses DHCP). L'étendue des adresses DHCP est spécifiée dans ce champ.
  - Client Lease Time (Durée de bail du client). Entrez le nombre de minutes dans ce champ.
- Time Setting (Réglage de l'heure). Ce paramètre vous permet de spécifier le fuseau horaire de votre passerelle.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

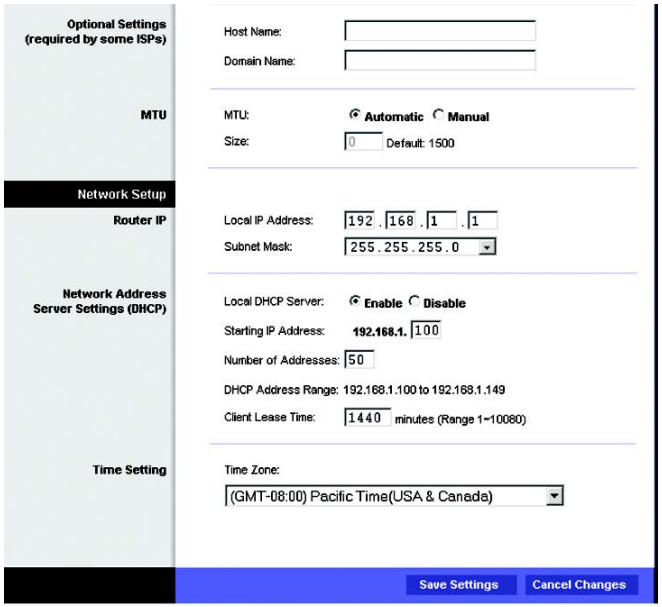

Figure 5-9 : Optional Settings (Paramètres facultatifs)

Onglet DDNS

La passerelle inclut une fonction DDNS (Dynamic Domain Name System). Cette fonction vous permet d'attribuer un nom de domaine et d'hôte fixe à une adresse IP Internet dynamique. Cela peut s'avérer utile si vous hébergez votre propre site Web, un serveur FTP ou tout autre type de serveur derrière la passerelle.

Avant d'opter pour cette fonctionnalité, vous devez obtenir la connexion à un service DDNS à l'adresse DynDNS.org.

DDNS

DDNS Service (Service DDNS). Si votre service DDNS est fourni par DynDNS.org, sélectionnez **DynDNS.org** dans le menu déroulant. (figure 5-10.) Pour désactiver le service DDNS, sélectionnez **Disabled** (Désactivé).

DynDNS.org

- User Name (Nom d'utilisateur), Password (Mot de passe) et Host Name (Nom d'hôte). Entrez le nom d'utilisateur, le mot de passe et le nom d'hôte du compte configuré avec DynDNS.org.
- Internet IP Address (Adresse IP Internet). L'adresse IP Internet actuelle de la passerelle est spécifiée dans ce champ. Puisqu'elle est dynamique, cette adresse change.
- Status (Etat). L'état de la connexion du service DDNS est spécifié dans ce champ.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-10 : DynDNS.org

Onglet Advanced Routing (Routage avancé)

L'écran Advanced Routing (Routage avancé) vous permet de configurer les paramètres de routage dynamique et de routage statique. (figure 5-11)

Advanced Routing (Routage avancé).

- Dynamic Routing (Routage dynamique). Le routage dynamique vous permet d'exiger de la passerelle qu'elle s'adapte aux modifications physiques de la configuration du réseau. La passerelle, à l'aide du protocole RIP, détermine l'itinéraire des paquets du réseau en fonction du plus petit nombre de sauts relevés entre la source et la destination. Le protocole RIP transmet régulièrement les informations de routage aux autres passerelles du réseau. Pour activer le RIP, cliquez sur **Enabled** (Activé). Pour désactiver le RIP, cliquez sur **Disabled** (Désactivé).
- Receive RIP Version (Version de réception RIP). Pour recevoir des messages RIP, sélectionnez le protocole souhaité : **RIP1** ou **RIP2**. Si vous ne souhaitez pas recevoir de messages RIP, sélectionnez **None** (Aucun).
- Transmit RIP Version (Version de transmission RIP). Pour transmettre des messages RIP, sélectionnez le protocole souhaité : **RIP1, RIP1-Compatible ou RIP2**. Si vous ne souhaitez pas transmettre de messages RIP, sélectionnez **None** (Aucun).

Static Routing (Routage statique)

Si la passerelle est connectée à plusieurs réseaux, il peut être nécessaire de définir un itinéraire statique entre eux. Un itinéraire statique est une voie prédéfinie que les informations du réseau doivent emprunter pour atteindre un hôte ou un réseau spécifique. Pour créer un itinéraire statique, modifiez les paramètres suivants :

- Select Entry (Sélectionner l'entrée). Sélectionnez le numéro de l'itinéraire statique dans le menu déroulant. La passerelle peut prendre en charge jusqu'à 20 entrées d'itinéraires statiques. Si vous souhaitez supprimer un itinéraire, une fois l'entrée sélectionnée, cliquez sur le bouton **Delete Entry** (Supprimer l'entrée).
- Destination IP Address (Adresse IP de destination). Cette option identifie l'adresse du réseau distant, ou hôte, auquel vous souhaitez attribuer un itinéraire statique. Entrez l'adresse IP de l'hôte pour lequel vous souhaitez créer un itinéraire statique. Si vous créez un itinéraire pour l'intégralité du réseau, assurez-vous que la portion de réseau de l'adresse IP est définie à 0.
- Subnet Mask (Masque de sous-réseau). Cette option, que l'on appelle également Masque de réseau, détermine la portion de l'adresse IP qui correspond au réseau et la portion de l'adresse IP qui correspond à l'hôte.
- Gateway (Passerelle). Il s'agit de l'adresse IP de la passerelle permettant le contact entre la passerelle et le réseau distant ou hôte.
- Hop Count (Comptage de tronçon). Cette option détermine le nombre maximal d'étapes entre les nœuds sur lesquels transitent les paquets de données. Un nœud est n'importe quel routeur se trouvant sur le chemin du réseau distant.

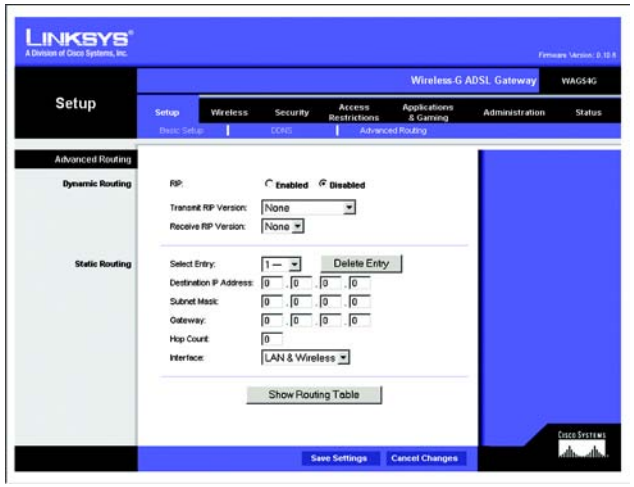

Figure 5-11 : Advanced Routing (Routage avancé)

- Interface (Interface). Sélectionnez **LAN & Wireless** (LAN et Sans fil) ou **Internet** (Internet) en fonction de l'emplacement de la destination finale de l'itinéraire statique.

- Show Routing Table (Afficher la table de routage). Cliquez sur le bouton **Show Routing Table** (Afficher la table de routage) pour afficher un écran (figure 5-12) indiquant l'itinéraire des données sur le réseau local (LAN). Pour chaque itinéraire, l'adresse IP de destination, le masque de sous-réseau, la passerelle et l'interface sont affichés. Cliquez sur le bouton **Refresh** (Actualiser) pour mettre à jour les informations.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

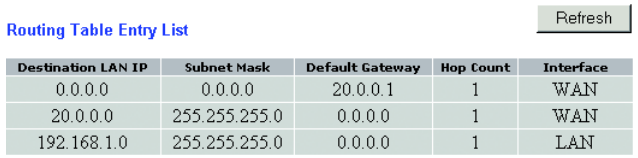

Figure 5-12 : Table de routage

Onglet Wireless (Sans fil)

Onglet Basic Wireless Settings (Paramètres sans fil de base) (figure 5-13)

Cet écran vous permet de sélectionner votre mode réseau sans fil ainsi que votre sécurité sans fil.

Wireless Network (Réseau sans fil)

- Wireless Network Mode (Mode réseau sans fil). Si votre réseau comporte des périphériques 802.11g et 802.11b, conservez le paramètre par défaut, **Mixed** (Mixte). Si votre réseau ne comporte que des périphériques 802.11g, sélectionnez l'option **802.11g**. Si votre réseau ne comporte que des périphériques 802.11b, sélectionnez l'option **802.11b**. Si vous souhaitez désactiver la gestion de réseau sans fil, sélectionnez **Disable** (Désactivé).

- Wireless Network Name (Nom du réseau sans fil ou SSID). Entrez le nom de votre réseau sans fil dans ce champ. Il s'agit du nom de réseau que partagent tous les périphériques interconnectés à un réseau sans fil. Le nom SSID doit être identique pour tous les périphériques du réseau sans fil. Ce paramètre est sensible à la casse et ne doit pas comprendre plus de 32 caractères alphanumériques. Tous les caractères du clavier peuvent être utilisés. Linksys vous recommande de remplacer le nom SSID (linksys) par défaut par un nom unique de votre choix.

- Wireless Channel (Canal sans fil). Sélectionnez le canal approprié dans la liste fournie pour qu'il corresponde à vos paramètres réseau, entre 1 et 11 (Amérique du Nord). Tous les points de votre réseau sans fil doivent utiliser le même canal pour fonctionner correctement. Les clients sans fil Linksys détecteront automatiquement le canal sans fil de la passerelle.

- Wireless SSID Broadcast (Diffusion SSID sans fil). Lorsque des ordinateurs clients sans fil recherchent sur le réseau local des réseaux sans fil auxquels s'associer, ils détectent le SSID diffusé par le routeur. Pour diffuser le SSID du routeur, conservez le paramètre par défaut **Enabled** (Activé). Si vous ne souhaitez pas diffuser le SSID du routeur, sélectionnez **Disabled** (Désactivé).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Figure 5-13 : Wireless Network Mode (Mode réseau sans fil).

Onglet Wireless Security (Sécurité sans fil)

Les paramètres de la section Wireless Security (Sécurité sans fil) permettent de configurer la sécurité de votre réseau sans fil. Le routeur prend en charge quatre options en mode Sécurité sans fil : WPA Pre-Shared Key (clé WPA partagée), WPA RADIUS, RADIUS et WEP. WPA, acronyme de Wi-Fi Protected Access, désigne une norme de sécurité plus solide que le système de cryptage WEP. WEP est l'acronyme de Wired Equivalent Privacy et RADIUS l'acronyme de Remote Authentication Dial-In User Service. Ces quatre modèles font l'objet d'une description sommaire ci-après. Pour obtenir des instructions plus détaillées sur la configuration de la sécurité sans fil du routeur, consultez l'« Annexe B : Sécurité sans fil ».

Figure 5-14 : WPA Pre-Shared Key (Clé WPA partagée).

WPA Pre-Shared Key (Clé WPA partagée). Le système WPA vous propose une méthode de cryptage, TKIP, associée à des clés de cryptage dynamiques. Sélectionnez le type d'algorithme, soit **TKIP**. Entrez une clé partagée WPA composée de 8 à 32 caractères. Spécifiez ensuite une période de renouvellement des clés du groupe dans le champ Group Key Renewal (Renouvellement des clés du groupe) pour indiquer au routeur à quelle fréquence il doit changer les clés de cryptage. (figure 5-14)

WPA RADIUS. Cette option associe le système WPA à l'utilisation conjointe d'un serveur RADIUS. (à sélectionner uniquement lorsqu'un serveur RADIUS est connecté au routeur). Tout d'abord, sélectionnez le type d'algorithme WPA à utiliser, soit **TKIP**. Entrez l'adresse IP et le numéro de port du serveur RADIUS, ainsi qu'une clé partagée entre le routeur et le serveur. Spécifiez enfin un délai de renouvellement des clés dans le champ Key Renewal Timeout (Délai de renouvellement des clés) pour préciser au routeur la fréquence à laquelle il doit changer les clés de cryptage. (figure 5-15)

Figure 5-15 : WPA RADIUS

RADIUS. Cette option associe le système WEP à l'utilisation conjointe d'un serveur RADIUS. (à sélectionner uniquement lorsqu'un serveur RADIUS est connecté au routeur). Entrez d'abord l'adresse IP et le numéro de port du serveur RADIUS, ainsi qu'une clé partagée entre le routeur et le serveur dans le champ Shared Key (Clé partagée). Sélectionnez ensuite le niveau de cryptage WEP : **64 bits 10 hex digits** (64 bits et 10 chiffres hexadécimaux) ou **128 bits 26 hex digits** (128 bits et 26 chiffres hexadécimaux). Sélectionnez la clé par défaut à utiliser. Enfin, générez une clé WEP à partir de l'option Passphrase (Phrase mot de passe) ou entrez-la manuellement. (figure 5-16)

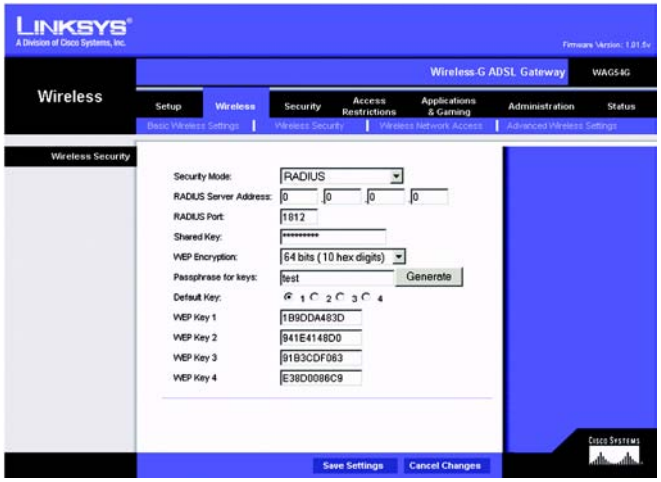

Figure 5-16 : RADIUS

WEP. Le système WEP est une méthode de cryptage de base qui n'est pas aussi sûre que le système WPA. Pour utiliser ce système, sélectionnez une clé par défaut (choisissez la clé à utiliser), puis un niveau de cryptage WEP : **64 bits 10 hex digits** (64 bits et 10 chiffres hexadécimaux) ou **128 bits 26 hex digits** (128 bits et 26 chiffres hexadécimaux). Générez ensuite une clé WEP à partir de l'option Passphrase (Phrase mot de passe) ou entrez-la manuellement. (figure 5-17)

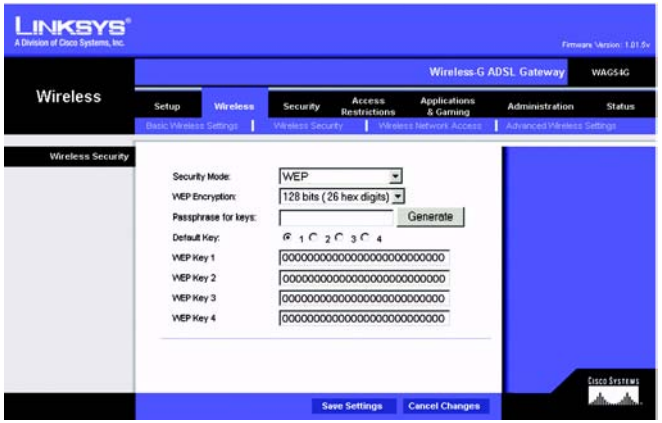

Figure 5-17 : WEP

- Modifiez ces paramètres comme décrit ci-contre, puis cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour appliquer vos modifications ou sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour obtenir des instructions plus détaillées sur la configuration de la sécurité sans fil du routeur, consultez l'« Annexe B : Sécurité sans fil ».
- WEP Encryption Level (Niveau de cryptage Web). Acronyme de Wired Equivalent Privacy, le WEP est une méthode de cryptage utilisée pour protéger vos communications sans fil. Le WEP utilise des clés 64 bits ou 128 bits pour contrôler l'accès à votre réseau et assurer la sécurité par le cryptage de chaque transmission de données. Pour décoder les données transmises, tous les périphériques d'un réseau doivent utiliser une clé WEP identique. Des niveaux de cryptage supérieurs offrent des niveaux de sécurité supérieurs mais, en raison de la complexité du cryptage, ils peuvent également diminuer les performances du réseau. Pour activer le WEP, sélectionnez **64 bits (10 hex digits)** (64 bits et 10 chiffres hexadécimaux) (figure 5-13) ou **128 bits (26 hex digits)** (128 bits et 26 chiffres hexadécimaux (figure 5-14).
- Passphrase for keys (Phrase mot de passe pour clés). Au lieu d'entrer manuellement les clés WEP, vous pouvez entrer une phrase mot de passe. Cette phrase mot de passe permet de générer une ou plusieurs clés WEP. Ce paramètre sensible à la casse ne doit pas comporter plus de 32 caractères alphanumériques. Cette fonction est compatible avec les produits sans fil Linksys uniquement et ne peut pas être utilisée avec l'utilitaire de configuration automatique de réseau sans fil de Windows XP. Si vous souhaitez communiquer avec des produits sans fil autres que des produits Linksys ou avec l'utilitaire de configuration automatique de réseau sans fil de Windows X, notez la clé WEP générée dans le champ WEP Key 1 (clé WEP 1) et entrez-la manuellement dans le client sans fil. Une fois la phrase mot de passe saisie, cliquez sur le bouton **Generate** (Générer) pour créer les clés WEP.
- Default Key (Clé par défaut). Sélectionnez la clé WEP (1-4) que vous souhaitez utiliser lorsque la passerelle transmet des données. Assurez-vous que le périphérique récepteur (client sans fil) utilise la même clé.
- WEP Keys 1-4 (Clés WEP 1-4). Les clés WEP vous permettent de créer un schéma de cryptage pour les transmissions réseau sans fil. Si vous n'utilisez pas de phrase mot de passe, entrez manuellement un ensemble de valeurs. Ne laissez aucun champ vierge et n'entrez pas de zéro, ce ne sont pas des valeurs de clés valides. Si vous utilisez un cryptage WEP 64 bits, la clé doit être constituée de 10 caractères hexadécimaux exactement. Si vous utilisez un cryptage WEP 128 bits, la clé doit être constituée de 26 caractères hexadécimaux exactement. Les caractères hexadécimaux valides sont : « 0 à 9 » et « A à F ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Wireless Network Access (Accès réseau sans fil) (figure 5-18)

Wireless Network Access (Accès réseau sans fil). Si vous sélectionnez **Allow All** (Tout autoriser), tous les ordinateurs sont autorisés à accéder au réseau sans fil. Pour restreindre l'accès au réseau, sélectionnez **Restrict Access** (Restreindre l'accès). Cliquez sur le bouton **Select MAC Address From Networked Computers** (Sélectionner l'adresse MAC à partir des ordinateurs du réseau) et l'écran représenté à la figure 5-19 apparaît.

Sélectionnez l'adresse **MAC Address** (Adresse MAC) dans la liste et cochez la case **Select** (Sélectionner), puis cliquez sur le bouton **Select** (Sélectionner).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran. Cliquez sur le bouton **Close** (Fermer) pour revenir à l'écran précédent.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

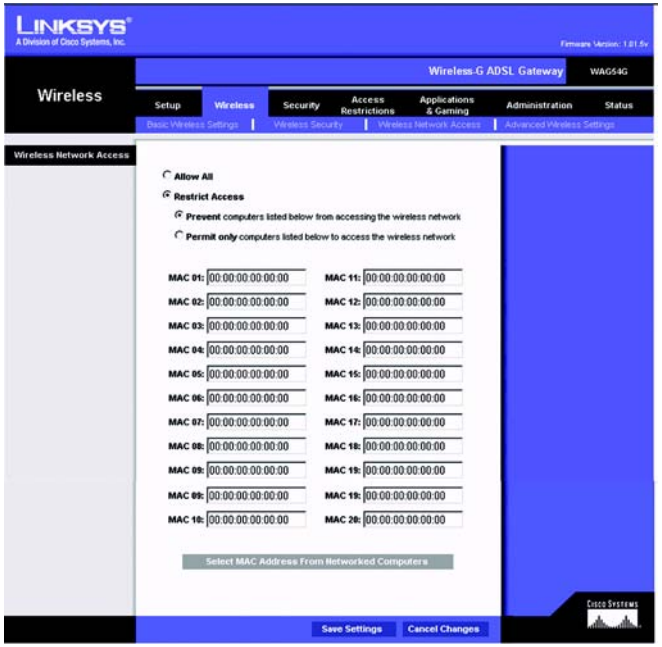

Figure 5-18 : Wireless Network Access (Accès réseau sans fil)

Figure 5-19 : Ordinateurs réseau

Onglet Advanced Wireless Settings (Paramètres sans fil avancés) (figure 5-20)

Cet écran vous permet d'accéder aux paramètres sans fil avancés dont Authentication Type (Type d'authentification), Basic Data Rates (Débits de données de base), Control Tx Rates (Débits Tx de contrôle), Beacon Interval (Intervalle de transmission de balise), DTIM Interval (Intervalle DTIM), RTS Threshold (Seuil RTS) et Fragmentation Threshold (Seuil de fragmentation).

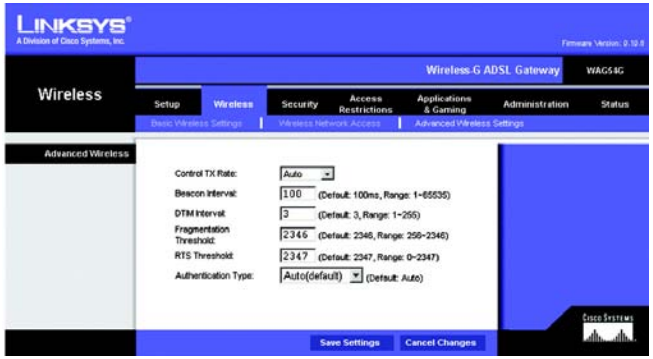

Figure 5-20 : Advanced Wireless Settings (Paramètres sans fil avancés)

- Control Tx Rates (Débits Tx de contrôle). Le débit de transmission par défaut est Auto (Auto). L'étendue est de 1 à 54 Mbit/s. Vous devez définir le taux de transmission des données en fonction de la vitesse de votre réseau sans fil. Vous pouvez faire votre choix parmi les diverses vitesses de transmission proposées ou sélectionner l'option **Auto** pour demander à la passerelle d'adopter automatiquement le taux de transmission le plus rapide possible et activer la fonctionnalité de reconnexion automatique. Cette fonctionnalité est alors chargée de définir la meilleure vitesse de connexion possible entre la passerelle et un client sans fil.
- Beacon Interval (Intervalle de transmission de balise). La valeur par défaut est 100. Entrez une valeur comprise entre 1 et 65 535 millisecondes. La valeur Beacon Interval (Intervalle de transmission de balise) indique l'intervalle de fréquence de la balise. Une balise désigne un paquet diffusé par la passerelle pour synchroniser le réseau sans fil.
- DTIM Interval (Intervalle DTIM). La valeur par défaut est 3. Cette valeur, comprise, entre 1 et 255, indique l'intervalle du message d'indication de transmission de données (DTIM). Un champ DTIM est un champ de compte à rebours chargé d'informer les clients sur la prochaine fenêtre à utiliser pour consulter des messages de diffusion ou de multidiffusion. Après avoir mis en mémoire tampon les messages de diffusion ou de multidiffusion des clients qui lui sont associés, la passerelle transmet le DTIM suivant avec une valeur d'intervalle DTIM. Ses clients sont informés par les balises et se préparent à recevoir les messages de diffusion et de multidiffusion.
- Fragmentation Threshold (Seuil de fragmentation). Il est préférable de conserver la valeur par défaut de 2346. L'étendue est 256-2346 octets. Cette valeur permet de spécifier la taille maximale d'un paquet avant de fragmenter les données en plusieurs paquets. Si le taux d'erreur de paquet que vous rencontrez est élevé, vous pouvez légèrement augmenter le seuil de fragmentation. Un seuil de fragmentation trop bas peut se traduire par des performances faibles du réseau. Seule une petite modification de cette valeur est recommandée.
- RTS Threshold (Seuil RTS). Il est préférable de conserver la valeur par défaut de 2347. L'étendue est 0-2347 octets. Si vous faites face à un flux de données incohérent, seule une modification légère de la valeur est recommandée. Si un paquet du réseau apparaît plus petit que la taille prédéfinie du seuil RTS ; le mécanisme RTS/CTS n'est pas activé. La passerelle transmet des trames RTS (Request To Send, requête d'envoi de données) à une station de réception donnée et négocie l'envoi d'une trame de données. Après réception d'un signal RTS, la station sans fil répond par une trame CTS (Clear To Send) pour autoriser le début de la transmission.
- Authentication Type (Type d'authentification). La valeur Auto définie (par défaut) vous permet de choisir entre une authentification Open System (Système ouvert) ou Shared Key (Clé partagée). En mode d'authentification Open System (Système ouvert), l'expéditeur et le destinataire n'utilisent pas de clé WEP pour l'authentification mais peuvent utiliser le WEP pour le cryptage des données. Si vous souhaitez autoriser une authentification Open System (Système ouvert), sélectionnez **Open System** (Système ouvert). Pour l'authentification Shared Key (Clé partagée), l'expéditeur et le destinataire utilisent une clé WEP pour l'authentification et le cryptage des données. Si vous souhaitez uniquement utiliser l'authentification Shared Key (Clé partagée), sélectionnez **Shared Key** (Clé partagée). Il est recommandé de conserver cette option en mode par défaut (Auto), car certains clients ne peuvent pas être configurés pour l'authentification Shared Key (Clé partagée).

Onglet Security (Sécurité)

Pare-feu

Lorsque vous cliquez sur l'onglet Security (Securité), l'écran Firewall (Pare-feu) apparaît (figure 5-21). Cet écran permet de définir les options Filters (Filtres) et Block Wan Requests (Blocage des requêtes WAN). Les filtres bloquent certains types de données Internet ainsi que les requêtes Internet anonymes.

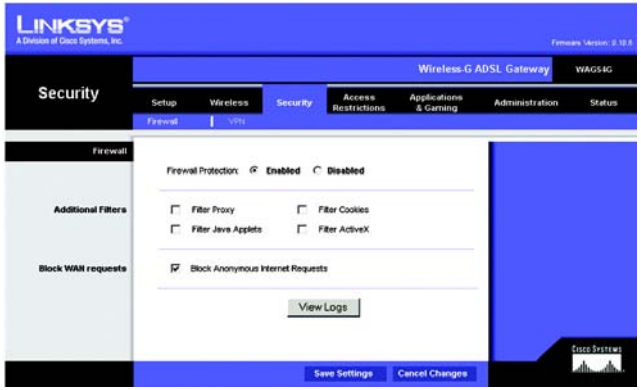

Figure 5-21 : Firewall (Pare-feu)

- Firewall (Pare feu). Pour sélectionner l'option Firewall Protection (Protection de pare-feu), cliquez sur **Enabled** (Activée). Si vous ne souhaitez pas sélectionner cette option, cliquez sur **Disabled** (Désactivée).

  Additional Filters (Filtres supplémentaires)

- Filter Proxy (Filtrer le proxy). L'utilisation de serveurs proxy WAN peut compromettre la sécurité de la passerelle. La suppression du filtre de proxy désactive l'accès aux serveurs de proxy WAN. Pour activer le filtre de proxy, cliquez sur **Enabled** (Activé).

- Filter Cookies (Filtrer les cookies). Un cookie est un ensemble de données stocké sur votre ordinateur et utilisé par les sites Internet lorsque vous consultez des pages Web. Pour activer le filtrage des cookies, cliquez sur **Enabled** (Activé).

- Filter Java Applets (Filtrer les Applets Java). Java est un langage de programmation pour sites Web. Si vous supprimez le filtrage des applets Java, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage des Applet Java, cliquez sur **Enabled** (Activé).

- Filter ActiveX (Filtrer ActiveX). ActiveX est un langage de programmation pour sites Web. Si vous supprimez le filtrage ActiveX, vous risquez de ne pas avoir accès aux sites Internet créés à l'aide de ce langage de programmation. Pour activer le filtrage ActiveX, cliquez sur **Enabled** (Activé).

  Block WAN Requests (Blocage des requêtes WAN)

- Block Anonymous Internet Requests (Blocage des requêtes Internet anonymes). Cette option permet à votre réseau de ne pas être détecté et renforce votre sécurité en cachant vos ports réseau. Les intrus auront ainsi plus de difficultés à découvrir votre réseau. Sélectionnez **Block Anonymous Internet Requests** (Bloquer les requêtes Internet anonymes). Pour autoriser ces requêtes, désélectionnez cette option.

Cliquez sur **View Logs** (Afficher les fichiers journaux) pour afficher le fichier journal de n'importe quel événement de pare-feu.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

VPN

VPN (Virtual Private Networking) est une mesure de sécurité qui crée une connexion sécurisée entre deux emplacements distants. L'écran VPN (figure 5-22) vous permet de configurer vos paramètres VPN afin d'améliorer la sécurité de votre réseau.

VPN Passthrough (Intercommunication VPN)

- IPSec Passthrough (Intercommunication IPSec). La technologie IPSec (Internet Protocol Security) désigne une série de protocoles utilisés pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP. Pour activer l'option IPSec Passthrough (Intercommunication IPSec), cliquez sur le bouton **Enabled** (Activée). Pour désactiver l'option IPSec Passthrough (Intercommunication IPSec), cliquez sur le bouton **Disabled** (Désactivée).
- PPTP Passthrough (Intercommunication PPTP). L'intercommunication PPTP (Point-to-Point Tunneling Protocol) est la méthode utilisée pour activer les sessions VPN dans un serveur Windows NT 4.0 ou 2000. Pour activer l'option PPTP Passthrough (Intercommunication PPTP), cliquez sur le bouton **Enabled** (Activée). Pour désactiver l'option PPTP Passthrough (Intercommunication PPTP), cliquez sur le bouton **Disabled** (Désactivée).

IPSec VPN Tunnel (Tunnel VPN IPSec)

La passerelle VPN crée un tunnel, ou canal, entre deux points terminaux, ainsi les données ou informations transitant entre ces deux points terminaux sont sécurisées.

- Pour établir ce tunnel, sélectionnez le tunnel que vous voulez créer dans la liste déroulante Select Tunnel Entry (Sélectionner une entrée de tunnel). Vous pouvez créer jusqu'à 5 tunnels simultanés. Cliquez ensuite sur **Enabled** (Activé) pour activer le tunnel VPN IPSec. Une fois le tunnel activé, donnez-lui un nom dans le champ Tunnel Name (Nom du tunnel). Ceci vous permet d'identifier les divers tunnels et il n'est donc pas nécessaire que ce nom corresponde au nom utilisé à l'autre bout du tunnel.
- Local Secure Group (Groupe sécurisé local) et Remote Secure Group (Groupe sécurisé distant). Local Secure Group (Groupe sécurisé local) correspond à l'ordinateur ou aux ordinateurs de votre réseau local (LAN) pouvant accéder au tunnel. Remote Secure Group (Groupe sécurisé distant) correspond à l'ordinateur ou aux ordinateurs du côté distant du tunnel pouvant accéder au tunnel. Ces ordinateurs peuvent être spécifiés par un sous-réseau, une adresse IP spécifique ou une étendue.
- Remote Security Gateway (Passerelle de sécurité distante). Remote Security Gateway (Passerelle de sécurité distante) correspond au périphérique VPN, tel qu'une deuxième passerelle, du côté distant du tunnel VPN. Renseignez les champs IP Address (Adresse IP) et Domain (Domaine) pour le périphérique VPN se trouvant de l'autre côté du tunnel. Le périphérique VPN distant peut être une autre passerelle VPN, un serveur VPN ou un ordinateur exécutant un logiciel client VPN prenant en charge IPSec. L'adresse IP peut être statique (permanente) ou dynamique (changeante) selon les paramètres du périphérique VPN distant. Vérifiez que vous avez saisi correctement l'adresse IP. Sinon la connexion ne peut pas être établie. Gardez à l'esprit qu'il ne s'agit PAS de l'adresse IP de la passerelle locale, mais de l'adresse IP de la passerelle ou du périphérique VPN distant avec lequel vous voulez communiquer. Si vous entrez une adresse IP, seule l'adresse IP spécifique pourra accéder au tunnel. Si vous sélectionnez **Any** (Toutes), toutes les adresses IP peuvent accéder au tunnel.

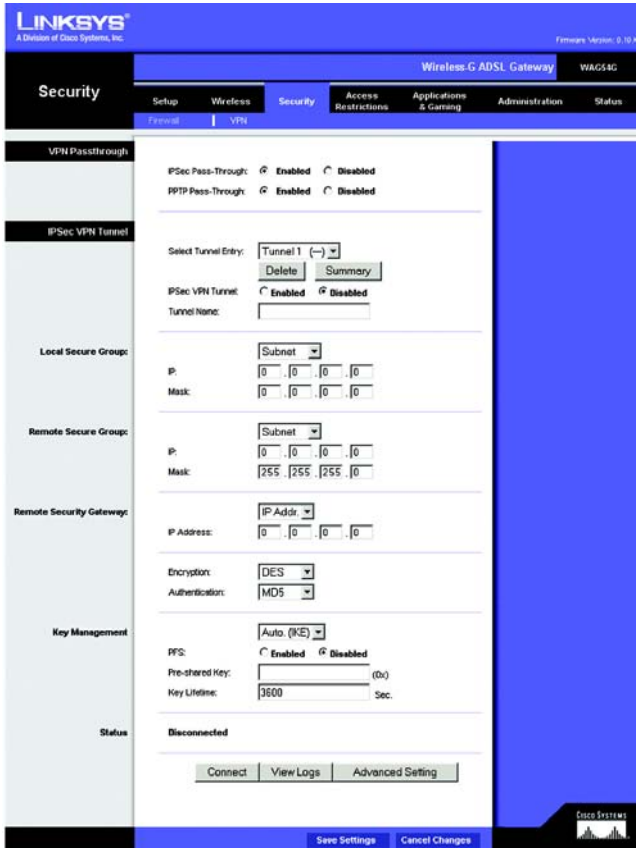

Figure 5-22 : VPN

- Encryption (Cryptage). Le paramètre Encryption (Cryptage) permet de sécuriser davantage votre connexion. Il existe deux types de cryptage : DES ou 3DES (3DES est le paramètre recommandé car il garantit un niveau de protection plus élevé). Vous pouvez sélectionner l'un de ces deux paramètres, mais le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel. Vous pouvez également ne pas souhaiter utiliser de cryptage. Dans ce cas, sélectionnez l'option Disable (Désactiver). A la figure 5-19, DES (paramètre par défaut) a été sélectionné.
- Authentication (Authentification). L'authentification constitue un niveau de sécurité supplémentaire. Il existe deux types d'authentification : MD5 et SHA. SHA est le paramètre recommandé car il garantit un niveau de protection plus élevé. Comme pour le cryptage, vous pouvez sélectionner l'un de ces deux paramètres, mais le même type d'authentification doit être utilisé par le périphérique VPN à l'autre bout du tunnel. L'authentification peut également être désactivée des deux côtés du tunnel, à l'aide du paramètre Disable (Désactiver). A la figure 5-19, MD5 (paramètre par défaut) a été sélectionné.
- Key Management (Gestion de clé). Sélectionnez **Auto (IKE)** (Auto (IKE)) ou **Manual** (Manuelle) dans le menu déroulant. Les deux méthodes sont décrites ci-dessous. Auto (IKE)
  Sélectionnez **Auto (IKE)** (Auto (IKE)) et saisissez une suite de chiffres ou de lettres dans le champ Pre-shared Key (Clé partagée). Une clé est générée sur la base de ce mot, qui DOIT être saisi des deux côtés du tunnel si cette méthode de cryptage est utilisée. Elle permet de crypter les données transmises par le tunnel et de les décrypter à l'autre bout du tunnel. Ce champ peut être renseigné à l'aide d'une combinaison de chiffres et de lettres de 24 caractères maximum. Les caractères spéciaux ou les espaces ne sont pas autorisés. Dans le champ Key Lifetime (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé. Saisissez la durée de validité de la clé en secondes ou laissez ce champ vierge pour que la clé reste valide indéfiniment. Cochez la case correspondant à l'option PFS (Perfect Forward Secrecy, Secret de transmission total) pour vous assurer que l'échange de clé et les propositions IKE sont sécurisées.

  Manual (Manuelle) (figure 5-23)
  Sélectionnez **Manual** (Manuelle) puis l'algorithme de cryptage souhaité dans le menu déroulant. Entrez la clé de cryptage dans le champ Encryption Key (Clé de cryptage). Si vous avez sélectionné DES pour votre algorithme de cryptage, entrez 16 caractères hexadécimaux. Si vous avez sélectionné 3DES, entrez 48 caractères hexadécimaux. Sélectionnez l'algorithme souhaité dans le menu déroulant Authentication Algorithm (Algorithme d'authentification). Entrez la clé d'authentification dans le champ Authentication Key (Clé d'authentification). Si vous avez sélectionné MD5 pour votre algorithme d'authentification, entrez 32 caractères hexadécimaux. Si vous avez sélectionné SHA1, entrez 40 caractères hexadécimaux. Entrez les données souhaitées dans les champs Inbound SPIs (SPIs entrants) et Outbound SPIs (SPIs sortants).
- Status (Etat). Ce paramètre indique l'état de la connexion.

Cliquez sur le bouton **Connect** (Connecter) pour connecter votre tunnel VPN. Cliquez sur le bouton View Logs (Afficher les fichiers journaux) pour afficher les fichiers journaux. Cliquez sur le bouton **Advanced Setting** (Paramètres avancés). L'écran de configuration du tunnel VPN IPSec apparaît. (figure 5-20).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

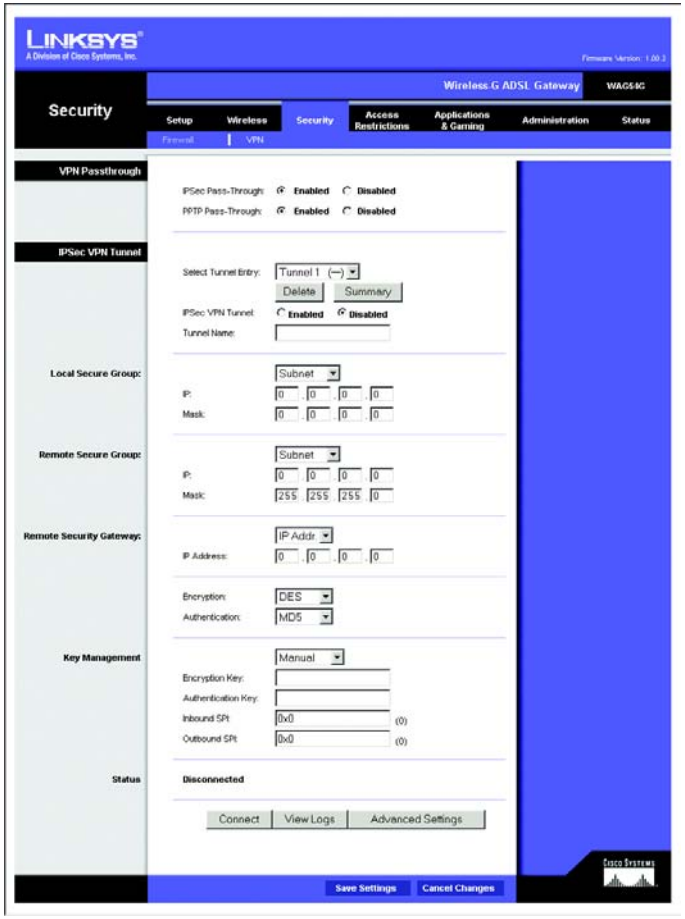

Figure 5-23 : Gestion de clé manuelle

Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec)

L'écran Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec) présenté à la figure 5-24, vous permet de définir les paramètres de tunnels VPN spécifiques.

Phase 1 (Phase 1)

- Cette phase permet de créer une association de sécurité (SA) souvent appelée IKE SA. Une fois la Phase 1 (Phase 1) terminée, la Phase 2 (Phase 2) permet de créer une ou plusieurs IPSec SA, qui sont ensuite utilisées dans les sessions de clés IPSec.
- Operation Mode (Mode de fonctionnement). Il existe deux modes de fonctionnement : Main (Principal) et Aggressive (Agressif). Ils peuvent échanger les mêmes charges IKE en différentes séquences. Le mode Main (Principal) est le plus utilisé. Néanmoins, certains utilisateurs préfèrent le mode Aggressive (Agressif) car il est plus rapide. Le mode Main (Principal) est destiné à utilisation normale et inclut plus de requêtes d'authentification que le mode Aggressive (Agressif). Le mode Main (Principal) est recommandé car il est plus sûr. Quel que soit le mode sélectionné, la passerelle VPN acceptera les requêtes Main (Principal) et Aggressive (Agressif) du périphérique VPN distant. Cochez la case Username (Nom d'utilisateur) puis entrez le nom d'utilisateur.
- Encryption (Cryptage). Sélectionnez la longueur de la clé utilisée pour crypter/décrypter les paquets ESP. Vous avez deux choix : DES et 3DES.3DES est recommandé car il est plus sûr.
- Authentication (Authentification). Sélectionnez la méthode utilisée pour authentifier les paquets ESP. Vous avez deux choix : MD5 et SHA. SHA est recommandé car il est plus sûr.
- Group (Groupe). Vous pouvez choisir entre deux groupes Diffie-Hellman : 768-bit (768 bits) et 1024-bit (1024 bits). Diffie-Hellman se réfère à une technique de cryptographie utilisée par les clés publiques et privées pour le cryptage et le décryptage.
- Key Life Time (Durée de validité de la clé). Dans le champ Key Lifetime (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé (facultatif). Entrez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

Phase 2 (Phase 2)

- Encryption (Cryptage). La méthode de cryptage sélectionnée à la Phase 1 (Phase 1) s'affiche à l'écran.
- Authentication (Authentification). La méthode d'authentification sélectionnée à la Phase 1 (Phase 1) s'affiche à l'écran.
- PFS. L'état du PFS s'affiche à l'écran.
- Group (Groupe). Vous pouvez choisir entre deux groupes Diffie-Hellman : 768-bit (768 bits) et 1024-bit (1024 bits). Diffie-Hellman se réfère à une technique de cryptographie utilisée par les clés publiques et privées pour le cryptage et le décryptage.

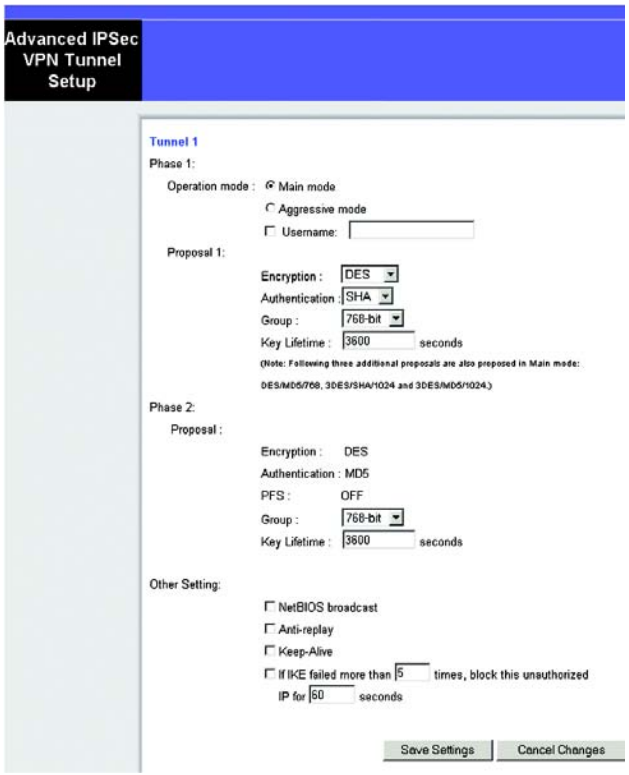

Figure 5-24 : Advanced IPSec VPN Tunnel Setup (Configuration avancée du tunnel VPN IPSec)

- Key Life Time (Durée de validité de la clé). Dans le champ Key Lifetime (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé. Entrez la durée de validité de la clé en secondes avant la prochaine renégociation de clé entre chaque point terminal.

Other Setting (Autres paramètres)

- NetBIOS broadcast (Diffusion NetBIOS). Cochez cette case pour permettre au trafic NetBIOS de passer par le tunnel VPN.

- Anti-replay (Anti-reprise) Cochez cette case pour activer la protection Anti-replay (Anti-reprise). Cette fonctionnalité effectue un suivi des séquences à l'arrivée des paquets, assurant ainsi la sécurité au niveau des paquets IP.

- Keep-Alive (Activée). Si vous sélectionnez cette option, la passerelle procède régulièrement à une vérification de votre connexion Internet. Si vous êtes déconnecté, la passerelle rétablit automatiquement votre connexion.

- Cochez cette case pour bloquer les adresses IP non autorisées. Dans le champ prévu à cet effet, spécifiez combien de fois IKE peut échouer avant le blocage de toutes les adresses IP non autorisées. Entrez cette durée en secondes.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler. Pour plus d'informations sur cet onglet, cliquez sur le bouton **Help** (Aide).

Onglet Access Restrictions (Restrictions d'accès)

Internet Access (Accès Internet)

L'onglet Access Restrictions (Restrictions d'accès) présenté à la figure 5-25, vous permet de bloquer ou d'autoriser certains types d'utilisations Internet. Vous pouvez définir vos stratégies d'accès à Internet pour des ordinateurs spécifiques et définir des filtres en utilisant les numéros de ports du réseau.

- Internet Access Policy (Stratégie d'accès à Internet). L'option Multiple Filters (Filtres multiples) peut être enregistrée sous les paramètres Internet Access Policies (Stratégies d'accès à Internet). Pour modifier une stratégie, sélectionnez son numéro dans le menu déroulant. L'onglet qui apparaît contient les paramètres de cette stratégie. Si vous souhaitez supprimer cette stratégie, cliquez sur le bouton **Delete** (Supprimer). Pour afficher un récapitulatif de toutes les stratégies, cliquez sur le bouton **Summary** (Récapitulatif).

  Les récapitulatifs sont répertoriés dans cet écran (figure 50-26). Il contient le nom et les paramètres de chaque stratégie. Pour revenir à l'onglet Filters (Filtres), cliquez sur le bouton **Close** (Fermer).

- Enter Policy Name (Entrer le nom de la stratégie). Les stratégies sont créées à partir des champs présentés ici.

  Pour créer une stratégie d'accès à Internet :

1. Entrez le nom de la stratégie dans le champ Policy Name (Nom de la stratégie) prévu à cet effet. Sélectionnez **Internet Access** (Accès à Internet) dans Policy Type (Type de stratégie).

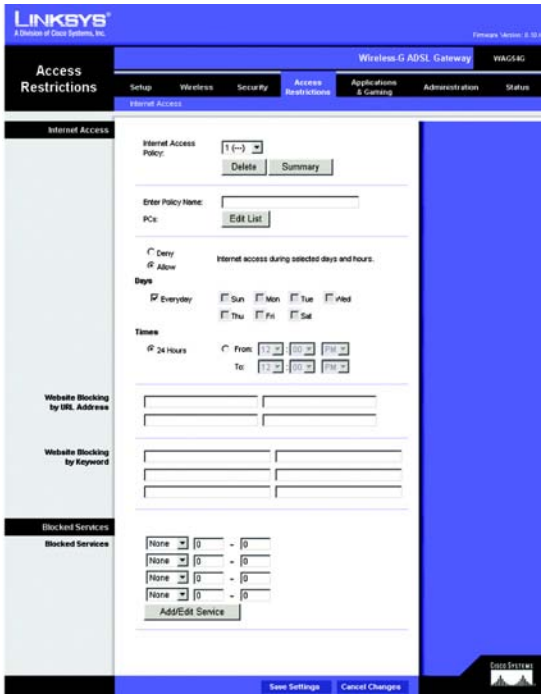

Figure 5-25 : Access Restriction (Restriction d'accès)

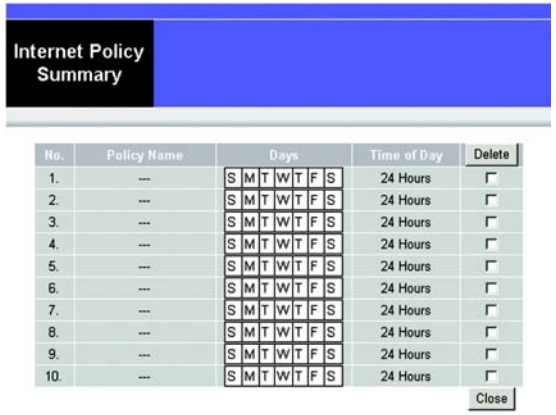
Internet Policy Summary
No.
Policy Name
Days
Time of Day
Delete
1. --- S M T W T F S 24 Hours
2. --- S M T W T F S 24 Hours
3. --- S M T W T F S 24 Hours
4. --- S M T W T F S 24 Hours
5. --- S M T W T F S 24 Hours
6. --- S M T W T F S 24 Hours
7. --- S M T W T F S 24 Hours
8. --- S M T W T F S 24 Hours
9. --- S M T W T F S 24 Hours
10. --- S M T W T F S 24 Hours
Close

Figure 5-26 : Internet Policy Summary (Récapitulatif de la stratégie Internet)

2. Cliquez ensuite sur le bouton **Edit List** (Modifier la liste). L'écran List of computers (Liste des ordinateurs) présenté à la figure 5-27, s'affiche à l'écran. Dans cet écran, vous pouvez entrer l'adresse IP ou l'adresse MAC de tous les ordinateurs auxquels la stratégie s'applique. Vous pouvez même entrer une étendue d'ordinateurs par adresse IP. Cliquez sur le bouton **Apply** (Appliquer) pour enregistrer vos paramètres. Le bouton **Cancel** (Annuler) vous permet d'annuler les modifications effectuées et le bouton **Close** (Fermer) de revenir à l'onglet Filters (Filtres).

3. Dans la liste de l'écran List of PCs (Liste des ordinateurs), cliquez sur Allow (Autoriser) pour autoriser l'accès Internet à des ordinateurs ou sur Deny (Refuser) pour le refuser.

4. Vous pouvez filtrer l'accès à divers services accessibles par Internet, notamment le service FTP ou Telnet, en choisissant un service dans les menus déroulants en regard de l'option Blocked Services (Services bloqués). Si un service n'est pas répertorié, vous pouvez cliquer sur le bouton **Add/Edit Service** (Ajouter/Modifier un service) pour ouvrir l'écran Port Services (Services des ports), présenté à la figure 5-28 et ajouter un service à la liste. Vous devrez alors renseigner les champs Service name (Nom du service), Protocol (Protocole) et Port Range (Connexion).

5. En choisissant les paramètres Days (Jours) et Time (Heure) appropriés, spécifiez la date et l'heure du filtrage d'accès à Internet.

6. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour activer la stratégie.

Il est également possible de filtrer l'accès à Internet par URL, c'est-à-dire l'adresse Internet permettant d'accéder à un site Web. Pour cela, entrez l'adresse URL souhaitée dans l'un des champs Website Blocking by URL Address (Blocage du site Web par adresse URL). Si vous ne connaissez pas l'adresse URL, vous pouvez effectuer un filtrage par mot-clé en entrant un mot-clé dans l'un des champs Website Blocking by Keyword (Blocage du site Web par mot-clé).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

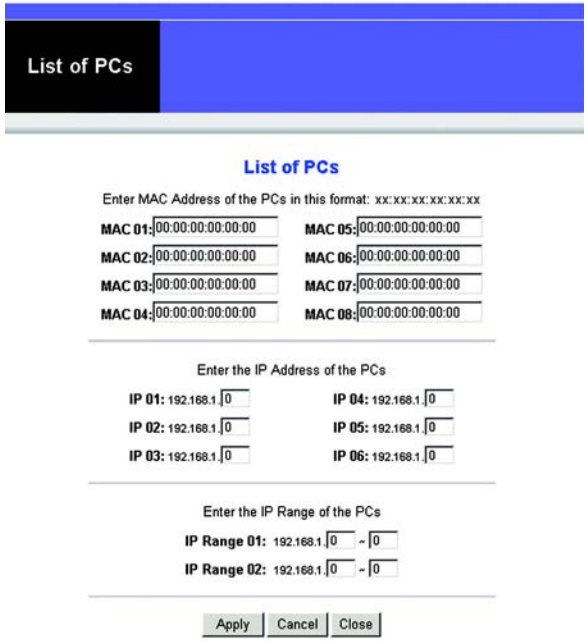

Figure 5-27 : List of PCs (Liste des ordinateurs)

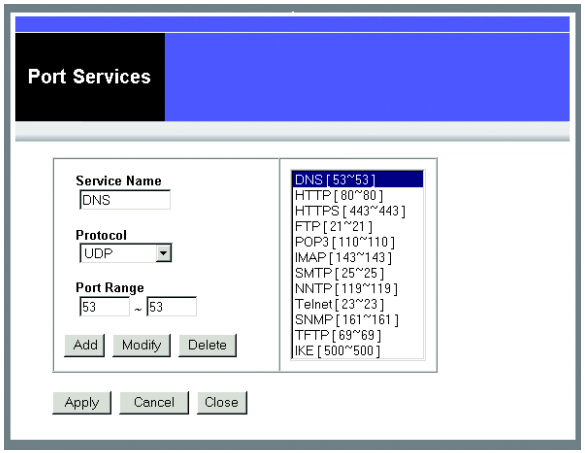

Figure 5-28 : Port Services (Services des ports)

Onglet Applications and Gaming (Applications et jeux)

Single Port Forwarding (Transfert de connexion unique)

Cet écran contient des options de personnalisation de vos services de ports pour les applications fréquemment utilisées. (figure 5-29).

Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, la passerelle transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

Sélectionnez ou entrez un nom d'application dans les champs prévus à cet effet. Entrez ensuite les numéros de ports internes et externes dans les champs External Port (Port externe) et Internal Port (Port interne). Sélectionnez le type de protocole que vous souhaitez utiliser pour chaque application : **TCP** ou **UDP**. Entrez l'adresse IP dans le champ IP Address (Adresse IP). Cliquez sur **Enabled** (Activé) pour activer le transfert UPnP pour les applications sélectionnées.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

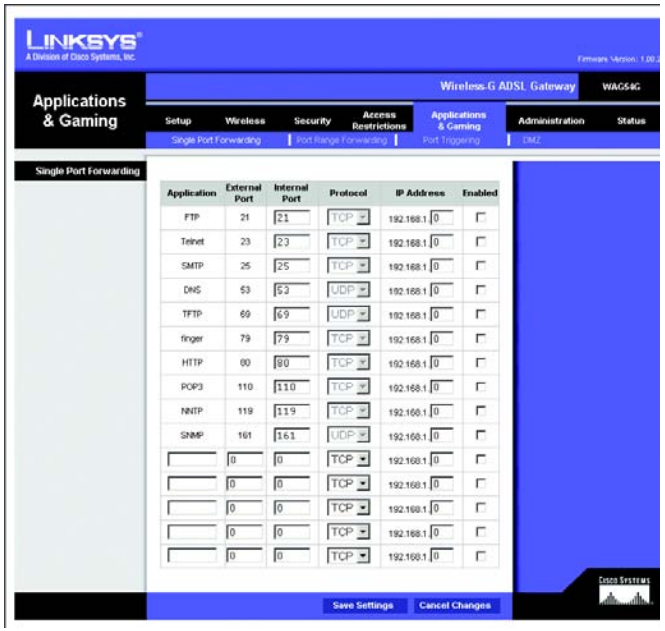

Figure 5-29 : Single Port Forwarding (Transfert de connexion unique)

Port Range Forwarding (Transfert de connexion)

Cet écran permet de configurer les services publics sur votre réseau, tels que les serveurs Web, les serveurs FTP, les serveurs de messagerie électronique ou toutes les autres applications Internet spécialisées. Par applications spécialisées, on entend toutes les applications qui utilisent un accès Internet pour effectuer des fonctions spécifiques, telles que la vidéoconférence ou les jeux en ligne. Certaines applications Internet peuvent n'exiger aucun transfert (figure 5-30).

Lorsque des utilisateurs envoient ce type de requête vers votre réseau via Internet, la passerelle transfère ces requêtes vers l'ordinateur approprié. Tout ordinateur dont le port est transféré doit avoir sa fonction de client DHCP désactivée et doit disposer d'une nouvelle adresse IP statique puisque son adresse IP risque de changer lors de l'utilisation de la fonction DHCP.

- Application (Application). Entrez le nom que vous souhaitez donner à chaque application.
- Start (Début) et End (Fin). Dans les champs Start (Début) et End (Fin), entrez les numéros de début et de fin du port que vous souhaitez transférer.
- TCP UDP. Sélectionnez le type de protocole que vous souhaitez utiliser pour chaque application : **TCP**, **UDP** ou **Both** (Les deux).
- IP Address (Adresse IP). Entrez l'adresse IP et cliquez sur **Enabled** (Activée).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

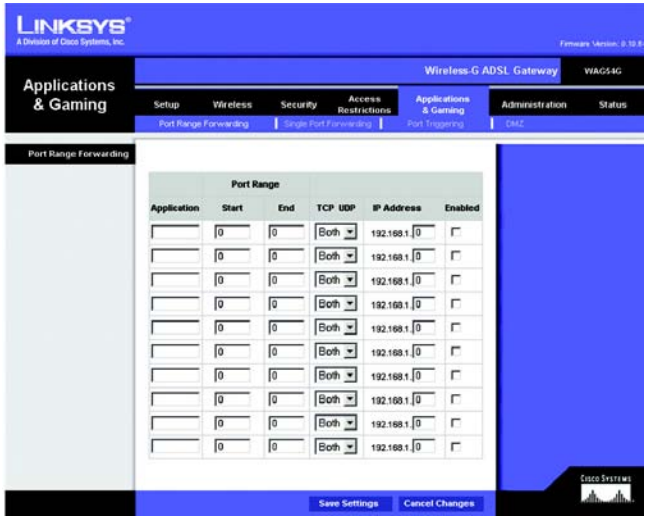

Figure 5-30 : Port Range Forwarding (Transfert de connexion)

Port Triggering (Déclenchement de connexion)

Le déclenchement de connexion est utilisé pour des applications spécifiques qui peuvent nécessiter l'ouverture d'un port à la demande. Pour cette fonction, la passerelle contrôle les données sortantes de certains numéros de ports spécifiques. (figure 5-31). La passerelle enregistre l'adresse IP de l'ordinateur qui envoie une requête de données. Ainsi lorsque les données transitent de nouveau par la passerelle, les données sont dirigées vers l'ordinateur approprié au moyen de l'adresse IP et des règles de mappage de ports.

- Application (Application). Entrez le nom que vous souhaitez donner à chaque application.
- Start Port (Port de début) et End Port (Port de fin). Aux sections Outgoing Triggered Range (Connexion sortante déclenchée) et Incoming Forwarded Range (Connexion entrante transférée), entrez vos informations dans les champs Start Port (Port de début) et End Port (Port de fin) pour le port que vous souhaitez transférer.

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

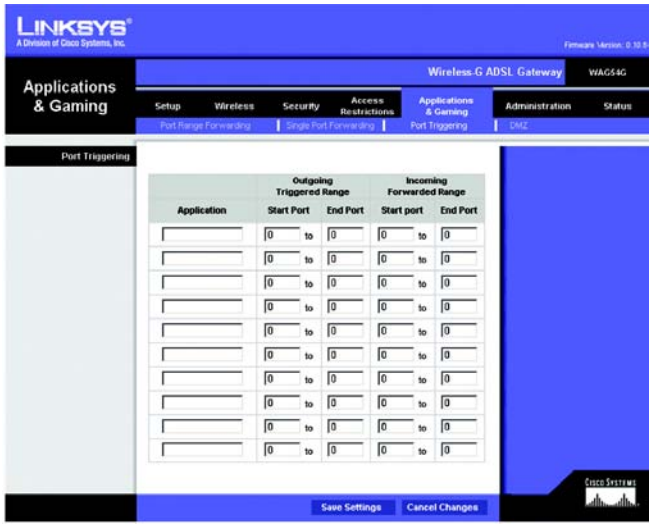

Figure 5-31 : Port Triggering (Déclenchement de connexion)

DMZ

L'écran DMZ (figure 5-32) permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence via l'hébergement DMZ. L'hébergement DMZ transfère simultanément tous les ports d'un ordinateur, à la différence de l'option Port Range Forwarding (Transfert de connexion) qui ne permet de transférer que 10 connexions au maximum.

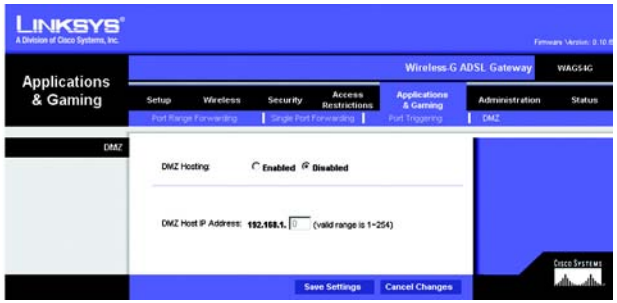

Figure 5-32 : DMZ

- DMZ Hosting (Hébergement DMZ). Cette fonctionnalité permet à un utilisateur local d'accéder à Internet en vue d'utiliser un service à usage spécifique, tel que des jeux Internet ou un système de vidéoconférence. Pour activer cette fonctionnalité, sélectionnez **Enabled** (Activé). Pour la désactiver, sélectionnez **Disabled** (Désactivé).

- DMZ Host IP Address (Adresse IP d'hôte DMZ). Pour exposer un ordinateur, entrez l'adresse IP de cet ordinateur. Pour obtenir l'adresse IP d'un ordinateur, reportez-vous à l'« Annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Onglet Administration (Administration)

Management (Gestion)

L'écran Management (Gestion), présenté à la figure 5-33, vous permet de modifier les paramètres d'accès à la passerelle et de configurer le protocole SNMP (Simple Network Management Protocol) ainsi que la fonctionnalité UPnP (Universal Plug and Play).

Figure 5-33 : Management (Gestion)

Gateway Access (Accès à la passerelle)

Local Gateway Access (Accès local à la passerelle). Pour assurer la sécurité de la passerelle, vous devez entrer un mot de passe pour accéder à l'utilitaire Web de la passerelle. Le nom d'utilisateur et le mot de passe par défaut est admin.

- Gateway Username (Nom d'utilisateur de la passerelle). Entrez le nom d'utilisateur par défaut : **admin**. Il est recommandé de remplacer ce nom d'utilisateur par défaut par un nom de votre choix.
- Gateway Password (Mot de passe de la passerelle). Il est recommandé de remplacer ce mot de passe par défaut par un mot de passe de votre choix.
- Re-enter to confirm (Confirmation du mot de passe). Entrez de nouveau le nouveau mot de passe de la passerelle pour le confirmer.

Remote Gateway Access (Accès distant à la passerelle). Cette fonction vous permet d'accéder à la passerelle à partir d'un emplacement distant, via Internet.

IMPORTANT : L'activation de l'administration à distance permet à chaque personne disposant de votre mot de passe de configurer à distance la passerelle via Internet.

- Remote Administration (Administration à distance). Cette fonction vous permet d'administrer la passerelle à partir d'un emplacement distant, via Internet. Pour activer l'administration à distance, cliquez sur **Enabled** (Activé).
- Administration Port (Port d'administration). Entrez le numéro de port que vous souhaitez utiliser pour accéder à distance à la passerelle.

SNMP

SNMP est un protocole très répandu de contrôle et de gestion réseau.

Identification (Identification). Pour activer le SNMP, cliquez sur **Enabled** (Activé). Pour désactiver le SNMP, cliquez sur **Disabled** (Désactivé).

- Dans le champ Device Name (Nom du périphérique), entrez le nom de la passerelle.

- Get Community (Obtenir la communauté). Entrez le mot de passe permettant l'accès en lecture seule aux informations SNMP de la passerelle.
- Set Community (Définir la communauté). Entrez le mot de passe permettant l'accès en lecture/écriture aux informations SNMP de la passerelle.

UPnP

UPnP permet à Windows XP de configurer automatiquement la passerelle pour diverses applications Internet, telles que des jeux Internet ou un système de vidéoconférence.

UPnp. Pour activer la fonctionnalité UPnP, cliquez sur **Enabled** (Activée).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Reporting (Rapports)

L'onglet Reporting (Rapports), présenté à la figure 5-34, vous fournit un fichier journal de toutes les URL ou adresses IP entrantes et sortantes de votre connexion Internet. Il fournit également des fichiers journaux de tous les événements VPN et de pare-feu.

Figure 5-34 : Reporting (Rapports)

Log (Fichier journal)

Log (Fichier journal). Pour activer la génération de fichiers journaux, cliquez sur **Enabled** (Activée).

- Logviewer IP Address (Adresse IP de réception des fichiers journaux). Entrez l'adresse IP de réception des fichiers journaux.

Email Alerts (Alertes de messagerie électronique)

E-Mail Alerts (Alertes de messagerie électronique). Pour activer les alertes de messagerie électronique, cliquez sur **Enabled** (Activées).

- Denial of Service Thresholds (Seuils de refus de service). Entrez les seuils des événements que vous souhaitez recevoir.
- SMTP Mail Server (Serveur de messagerie électronique SMTP). Entrez l'adresse IP du serveur SMTP.
- E-Mail Address for Alert Logs (Adresse de messagerie électronique pour fichiers journaux d'alertes). Entrez l'adresse de messagerie électronique pour les fichiers journaux d'alertes.
- Return E-Mail address (Adresse de messagerie électronique de retour). Entrez l'adresse de retour des messages électroniques.

Pour afficher les fichiers journaux, cliquez sur le bouton **View Logs** (Afficher les fichiers journaux).

Une fois que vos modifications sont effectuées dans cet onglet, cliquez sur **Save Settings** (Enregistrer les paramètres) ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour les annuler.

Diagnostics (Diagnostics)

Ping Test (Test Ping) (figure 5-35).

Ping Test Parameters (Paramètres de test Ping)

- Ping Target IP (IP de cible Ping). Entrez l'adresse IP pour laquelle vous souhaitez effectuer le test Ping. Il peut s'agir d'une adresse IP locale (LAN) ou Internet (WAN).
- Ping Size (Taille de Ping). Entrez une taille de paquets Ping.
- No. of Pings (Nombre de Pings). Entrez le nombre de fois que vous souhaitez effectuer le Ping.
- Ping Interval (Intervalle de Ping). Entrez l'intervalle de Ping en millisecondes.
- Ping Timeout (Délai de Ping). Entrez le délai en millisecondes.
- Ping Result (Résultat de Ping). Les résultats du test de Ping sont affichés ici.

Cliquez sur le bouton **Start Test** (Démarrer le test) pour démarrer le test de Ping.

Figure 5-35 : Ping Test (Test Ping)

Factory Defaults (Paramètres d'usine) (figure 5-36).

Restore Factory Defaults (Restaurer les paramètres d'usine). Si vous avez essayé toutes les solutions et que vous souhaitez restaurer les paramètres d'usine de la passerelle (vous perdrez alors tous vos paramètres), cliquez sur **Yes** (Oui).

Pour débuter le processus de restauration, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer ces modifications ou cliquez sur le bouton **Cancel Changes** (Annuler les modifications) pour annuler les modifications effectuées.

Figure 5-36 : Factory Defaults (Paramètres d'usine)

Firmware Upgrade (Mise à jour du micrologiciel) (figure 5-37).

Pour mettre à niveau le micrologiciel de la passerelle :

1. Cliquez sur le bouton **Browse** (Parcourir) pour rechercher le fichier de mise à niveau du micrologiciel que vous avez téléchargé à partir du site Web international Linksys puis décompressé.

2. Double-cliquez sur le fichier du micrologiciel que vous venez de télécharger et de décompresser. Cliquez sur le bouton **Upgrade** (Mettre à niveau) et suivez les instructions à l'écran.

Figure 5-37 : Firmware Upgrade (Mise à niveau du micrologiciel)

L'onglet Status (Etat)

Gateway (Passerelle)

Cet écran contient des informations sur votre passerelle et ses connexions WAN (Internet). (figure 5-38).

Gateway Information (Informations sur la passerelle)

Cette section contient les éléments suivants : Software Version (Version du logiciel), MAC Address (Adresse Mac) et Current Time (Heure actuelle).

Internet Connections (Connexions Internet)

Cette section contient les éléments suivants : ADSL Link (Lien ADSL), PPP Login (Connexion PPP), Internet IP Address (Adresse IP Internet), Public Subnet Mask (Masque de sous-réseau public), Default Gateway (Passerelle par défaut), Primary DNS Server (Serveur DNS principal) et Internet DHCP IP Expires (IP DHCP Internet expire).

System Statistics (Statistiques système)

Cette section contient les éléments suivants : Packets Sent (Paquets envoyés) et Packets Received (Paquets reçus).

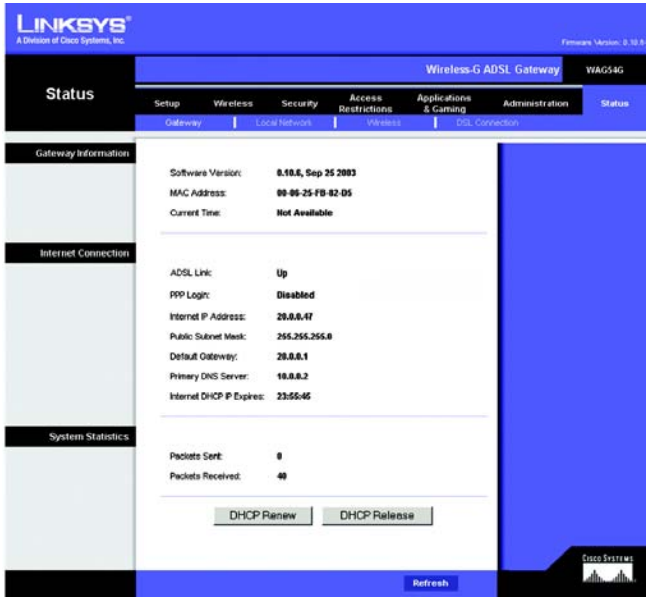

Figure 5-38 : Status (Etat)

DHCP Renew (Renouvellement DHCP). Cliquez sur le bouton **DHCP Renew** (Renouvellement DHCP) pour remplacer l'adresse IP actuelle de la passerelle par une nouvelle adresse IP.

DHCP Release (Version DHCP). Cliquez sur le bouton **DHCP Release** (Version DHCP) pour supprimer l'adresse IP actuelle de la passerelle.

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran.

Local Network (Réseau local)

Cette section contient les éléments suivants : Local Mac Address (Adresse Mac locale), IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau) et DHCP Server (Serveur SHCP). Pour afficher le tableau des clients DHCP, cliquez sur le bouton **DHCP Client Table** (Tableau des clients DHCP). (figure 5-39).

DHCP Client Table (Tableau des clients DHCP). Cliquez sur le bouton **DHCP Client Table** (Tableau des clients DHCP) pour afficher les données actuelles des clients DHCP. Ce tableau contient l'adresse Mac, le nom de l'ordinateur et l'adresse IP des clients réseau qui utilisent le serveur DHCP. Les données sont stockées dans la mémoire temporaire et sont régulièrement modifiées. (figure 5-40).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran.

Figure 5-39 : Local Network (Réseau local)

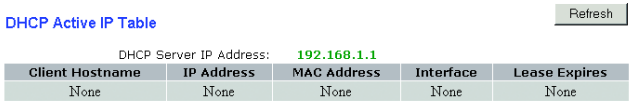

Figure 5-40 : Tableau des clients DHCP

Wireless (Sans fil)

Cette section contient les éléments suivants : Wireless Firmware Version (Version du micrologiciel sans fil), MAC Address (Adresse Mac), Status (Etat), Mode (Mode), Channel (Canal), SSID et Encryption (Cryptage). (figure 5-41).

Cliquez sur le bouton **Wireless Clients Connected** (Clients sans fil connectés) pour afficher les clients sans fil connectés à la passerelle.

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran.

Figure 5-41 : Wireless (Sans fil)

DSL Connection (Connexion DSL)

Cette section contient les éléments suivants : Status (Etat), Downstream Rate (Débit de réception), Upstream Rate (Débit d'émission), Encapsulation (Encapsulation), VPI, Vcl et Multiplexing (Multiplexage). (figure 5-42).

Cliquez sur le bouton **Refresh** (Actualiser) si vous souhaitez actualiser l'écran.

Figure 5-42 : DSL Connection (Connexion DSL)

Annexe A : Dépannage

Cette annexe est composée de deux sections, l'une abordant les problèmes courants et les solutions à y apporter, l'autre traitant des questions fréquemment posées. Des solutions envisageables pour les problèmes susceptibles de se produire lors de l'installation et de l'exploitation de la passerelle y sont décrites. Les descriptions ci-dessous vous aideront à résoudre vos problèmes. Si vous n'y trouvez aucune réponse, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Problèmes fréquents et solutions

1. ***Je souhaite définir une adresse IP statique sur un ordinateur.***
   Vous pouvez attribuer une adresse IP statique à un ordinateur en procédant comme suit :
   - Windows 98 et Windows Me :
     1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur **Réseau**.
     2. Dans la zone Les composants réseau suivants sont installés, sélectionnez le composant TCP/IP associé à votre adaptateur Ethernet. Si un seul adaptateur Ethernet est installé, une seule ligne TCP/IP apparaît sans association à un adaptateur Ethernet. Mettez-la en surbrillance, puis cliquez sur le bouton Propriétés.
     3. Dans la fenêtre Propriétés TCP/IP, sélectionnez l'onglet Adresse IP, puis l'option Spécifier une adresse IP. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté à la passerelle. Assurez-vous que chaque adresse IP est unique pour chaque ordinateur ou périphérique du réseau.
     4. Cliquez sur l'onglet **Passerelle**, puis tapez 192.168.1.1 dans le champ Nouvelle passerelle, c'est-à-dire l'adresse IP par défaut de la passerelle. Cliquez sur le bouton Ajouter pour valider cette entrée.
     5. Cliquez sur l'onglet **Configuration DNS** et assurez-vous que l'option Désactiver DNS est sélectionnée. Entrez les noms de l'hôte et du domaine (par exemple, « Jean » pour l'hôte et « domicile » pour le domaine). Entrez l'adresse DNS fournie par votre fournisseur d'accès Internet (FAI). Si votre FAI ne vous a fourni aucune adresse IP DNS, contactez-le ou consultez son site Web pour vous procurer cette information.
     6. Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur Fermer ou sur OK dans la fenêtre Réseau.
     7. Redémarrez l'ordinateur si le système vous y invite.
   - Windows 2000 :
     1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur **Connexions réseau et accès à distance**.
     2. Cliquez avec le bouton droit de la souris sur la Connexion au réseau local associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.
     3. Dans la zone Les composants sélectionnés sont utilisés par cette connexion, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance, puis sélectionnez l'option Propriétés. Sélectionnez l'option **Utiliser l'adresse IP suivante**.
     4. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté à la passerelle.
     5. Entrez le masque de sous-réseau 255.255.255.0.
     6. Entrez la passerelle par défaut 192.168.1.1 (adresse IP par défaut de la passerelle).

7. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis entrez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
8. Cliquez sur **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP), puis de nouveau sur **OK** dans la fenêtre Propriétés de Connexion au réseau local.
9. Redémarrez l'ordinateur si le système vous y invite.

- Windows XP :

  Les instructions ci-après supposent que vous utilisez l'interface par défaut de Windows XP. Si vous utilisez l'interface classique (dans laquelle les icônes et les menus se présentent comme dans les versions précédentes de Windows), suivez les instructions fournies pour Windows 2000.

  1. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
  2. Cliquez sur l'icône **Connexions réseau et Internet**, puis sur l'icône **Connexions réseau**.
  3. Cliquez à l'aide du bouton droit de la souris sur la **Connexion au réseau local** associée à l'adaptateur Ethernet que vous utilisez, puis sélectionnez l'option Propriétés.
  4. Dans la zone **Cette connexion utilise les éléments suivants**, mettez l'option **Protocole Internet (TCP/IP)** en surbrillance. Cliquez sur le bouton **Propriétés**.
  5. Entrez une adresse IP unique utilisée par aucun autre ordinateur du réseau connecté à la passerelle.
  6. Entrez le masque de sous-réseau 255.255.255.0.
  7. Entrez l'adresse IP par défaut de la passerelle : 192.168.1.1.
  8. Dans la partie inférieure de la fenêtre, sélectionnez l'option Utiliser l'adresse de serveur DNS suivante, puis entrez le serveur DNS préféré et le serveur DNS auxiliaire (fournis par votre FAI). Contactez votre FAI ou consultez son site Web pour vous procurer cette information.
  9. Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Protocole Internet (TCP/IP). Cliquez sur le bouton **OK** dans la fenêtre Propriétés de Connexion au réseau local.

2. Je souhaite tester ma connexion Internet.

A. Vérifiez vos paramètres TCP/IP.

Windows 98, Me, 2000 et XP :

- Pour obtenir des informations détaillées, reportez-vous au « Chapitre 4 : Connexion de la passerelle ADSL sans fil G ». Assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres.

Windows NT 4.0 :

- Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Cliquez deux fois sur l'icône **Réseau**.
- Cliquez sur l'onglet Protocole, puis double-cliquez sur le protocole TCP/IP.
- Dans la fenêtre qui s'affiche, assurez-vous que vous avez sélectionné l'adaptateur approprié et définissez-le à **Obtenir une adresse IP par un serveur DHCP**.
- Cliquez sur le bouton **OK** dans la fenêtre Propriétés TCP/IP, puis cliquez sur le bouton **Fermer** dans la fenêtre Réseau.
- Redémarrez l'ordinateur si le système vous y invite.

B. Ouvrez une invite de commande.

Windows 98 et Windows Me :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ Ouvrir, tapez command. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

Windows NT, 2000 et XP :

- Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ Ouvrir, tapez cmd. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**. Dans l'invite de commande, tapez ping 192.168.1.1, puis appuyez sur la touche Entrée.
- Si vous obtenez une réponse, cela signifie que l'ordinateur communique bel et bien avec la passerelle.
- Si vous n'obtenez PAS de réponse, vérifiez le câble et assurez-vous que l'option Obtenir une adresse IP automatiquement est sélectionnée dans les paramètres TCP/IP de votre adaptateur Ethernet.

C. Dans l'invite de commande, tapez la commande ping suivie de votre adresse IP Internet ou WAN, puis appuyez sur la touche **Entrée**. Vous pouvez vous procurer l'adresse IP Internet ou WAN dans l'écran Status (Etat) de l'utilitaire Web de la passerelle. Par exemple, si votre adresse IP Internet ou WAN est 1.2.3.4, vous devez entrer la commande ping 1.2.3.4, puis appuyez sur la touche Entrée.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté à la passerelle.
- Si vous n'obtenez PAS de réponse, essayez d'appliquer la commande Ping à partir d'un autre ordinateur pour vérifier si l'ordinateur d'origine est ou non la cause du problème.

D. Dans l'invite de commande, tapez ping www.yahoo.com, puis appuyez sur la touche **Entrée**.

- Si vous obtenez une réponse, cela signifie que l'ordinateur est connecté à Internet. Si vous ne parvenez pas à ouvrir une page Web, exécutez la commande Ping à partir d'un autre ordinateur pour vérifier si le premier ordinateur utilisé est ou non la cause du problème.
- Si vous n'obtenez PAS de réponse, le problème est peut-être lié à la connexion. Essayez d'appliquer la commande Ping à partir d'un autre ordinateur pour vérifier si l'ordinateur d'origine est ou non la cause du problème.

3. Je n'obtiens aucune adresse IP sur Internet par le biais de ma connexion Internet.

- Reportez-vous au « Problème 2 : Je souhaite tester ma connexion Internet » pour vérifier votre connectivité.
  1. Assurez-vous que vous utilisez les paramètres de connexion Internet adéquats. Contactez votre FAI pour savoir si votre connexion Internet est de type RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE ou RFC 2364 PPPoA. Reportez-vous à la rubrique Configuration du « Chapitre 5 : Configuration de la passerelle » pour obtenir des informations détaillées sur les paramètres de connexion Internet.
  2. Assurez-vous que vous disposez du câble approprié. Vérifiez si le voyant ADSL de la passerelle est allumé.
  3. Assurez-vous que le câble reliant le port ADSL de la passerelle est connecté à la prise murale ADSL. Vérifiez que la page Status (Etat) de l'utilitaire Web de la passerelle indique une adresse IP valide fournie par votre FAI.
  4. Eteignez l'ordinateur et la passerelle. Attendez 30 secondes puis allumez de nouveau la passerelle et l'ordinateur. Ouvrez l'onglet Status (Etat) de l'utilitaire Web de la passerelle pour contrôler que vous disposez bien d'une adresse IP.

4. Je ne parviens pas à accéder à la page de configuration de l'utilitaire Web de la passerelle.

- Reportez-vous au « Problème 2 : Je souhaite tester ma connexion Internet » pour vérifier que votre ordinateur est correctement connecté à la passerelle.

1. Reportez-vous à l'« Annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet » pour vérifier que votre ordinateur possède bien une adresse IP, un masque de sous-réseau, une passerelle et une adresse DNS.
2. Définissez une adresse IP statique sur votre système. Reportez-vous au « Problème 1 : Je souhaite définir une adresse IP statique sur un ordinateur. »
3. Reportez-vous au « Problème 10 : Je souhaite supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE). »

5. Mon VPN (Virtual Private Network) ne fonctionne pas via la passerelle.

Accédez à l'interface Web de la passerelle en spécifiant http://192.168.1.1 ou l'adresse IP de la passerelle, puis sélectionnez l'onglet Security (Sécurité). Assurez-vous que l'intercommunication IPsec et/ou l'intercommunication PPTP sont activées.

- Les VPN qui utilisent l'authentification IPSec avec ESP (Encapsulation Security Payload, qui porte également le nom de Protocole 50) fonctionnent alors correctement. Au moins une session IPSec fonctionne via la passerelle. Néanmoins, des sessions IPSec simultanées sont possibles, en fonction des spécifications de vos VPN.
- Les VPN qui utilisent IPSec et AH (Authentication Header, qui porte également le nom de Protocole 51) sont incompatibles avec la passerelle. AH est soumis à des limitations en raison d'une incompatibilité occasionnelle avec la norme NAT.
- Remplacez l'adresse IP de la passerelle par un autre sous-réseau, afin d'éviter les conflits entre l'adresse IP du VPN et votre adresse IP locale. Par exemple, si votre serveur VPN attribue une adresse IP 192.168.1.X (X étant un numéro entre 1 et 254) et que votre adresse IP LAN locale est 192.168.1.X (X étant le même numéro utilisé dans l'adresse IP VPN), la passerelle aura des difficultés à envoyer les informations vers l'emplacement correct. Si vous remplacez l'adresse IP de la passerelle par 192.168.2.1, le problème devrait être résolu. Changez l'adresse IP de la passerelle à l'aide de l'onglet Setup (Configuration) de l'interface Web.
- Si vous avez attribué une adresse IP statique à un ordinateur ou périphérique du réseau, vous devez remplacer son adresse IP par 192.168.2.Y (Y étant un nombre quelconque compris entre 1 et 254). Veuillez noter que chaque adresse IP doit être unique sur le réseau.
- Votre VPN peut exiger l'envoi de paquets port 500/UDP vers l'ordinateur connecté au serveur IPSec. Pour plus d'informations, reportez-vous au « Problème 7 : Je souhaite configurer un hébergement pour jeux en ligne ou utiliser d'autres applications Internet. »
- Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

6. Je souhaite configurer un serveur derrière ma passerelle et le rendre accessible au public.

Pour utiliser un serveur tel qu'un serveur de messagerie, Web ou FTP, vous devez connaître les numéros de port utilisés. Par exemple, le port 80 (HTTP) est utilisé pour le Web, le port 21 (FTP) pour le FTP et le port 25 (SMTP sortant) et le port 110 (POP3 entrant) pour la messagerie. Pour obtenir de plus amples informations, reportez-vous à la documentation fournie avec le serveur que vous avez installé.

- Pour configurer le transfert de connexion via l'utilitaire Web de la passerelle, procédez comme suit : Nous allons configurer des serveurs Web, FTP et de messagerie.
  1. Accédez à l'utilitaire Web de la passerelle en spécifiant http://192.168.1.1 ou l'adresse IP de la passerelle. Accédez à Applications and Gaming (Applications et jeux) - Onglet Port Range Forwarding (Transfert de connexion).

2. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
3. Entrez ensuite l'étendue des ports du service que vous utilisez. Par exemple, si vous utilisez un serveur Web, entrez l'étendue 80 à 80.
4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
5. Entrez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur du port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, entrez 100 dans le champ. Pour plus d'informations sur l'obtention d'une adresse IP, reportez-vous à l' « annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».
6. Cochez la case correspondant aux services de port que vous souhaitez utiliser. Voici un exemple :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
Serveur Web	80 à 80	X		192.168.1.100	X
Serveur FTP	21 à 21	X		192.168.1.101	X
SMTP (sortant)	25 à 25	X		192.168.1.102	X
POP3 (entrant)	110 à 110	X		192.168.1.102	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

7. Je souhaite configurer un hébergement pour jeux en ligne ou utiliser d'autres applications Internet.

Si vous souhaitez jouer en ligne ou utiliser des applications Internet, la plupart des opérations fonctionnent sans aucun transfert de connexion ou hébergement DMZ. Il se peut que vous souhaitiez héberger un jeu en ligne ou une application Internet. Vous devez dans ce cas configurer la passerelle pour qu'elle envoie les paquets entrants ou les données entrantes vers un ordinateur spécifique. Ceci s'applique également aux applications Internet que vous utilisez. Pour connaître les ports à utiliser, consultez directement le site Web des jeux en ligne ou des applications. Pour configurer l'hébergement de jeux en ligne ou utiliser une application Internet spécifique, procédez comme suit :

1. Accédez à l'interface Web de la passerelle en spécifiant http://192.168.1.1 ou l'adresse IP de la passerelle. Accédez à Applications and Gaming (Applications et jeux) - Onglet Port Range Forwarding (Transfert de connexion).
2. Entrez dans ce champ le nom que vous souhaitez donner à l'application personnalisée.
3. Entrez ensuite l'étendue des ports du service que vous utilisez. Par exemple, si vous souhaitez héberger Unreal Tournament (UT), entrez l'étendue 7777 à 27900.
4. Vérifiez le protocole que vous allez utiliser : TCP et/ou UDP.
5. Entrez l'adresse IP de l'ordinateur ou du périphérique réseau auquel vous souhaitez que le serveur de port accède. Par exemple, si l'adresse IP de l'adaptateur Ethernet du serveur Web est 192.168.1.100, entrez 100 dans le champ. Pour plus d'informations sur l'obtention d'une adresse IP, reportez-vous à l' « annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet ».
6. Cochez la **case correspondant aux services de port** que vous souhaitez utiliser. Voici un exemple :

Application personnalisée	Port externe	TCP	UDP	Adresse IP	Activer
UT	7777 à 27900	X	X	192.168.1.100	X
Halflife	27015 à 27015	X	X	192.168.1.105	X
PC Anywhere	5631 à 5631		X	192.168.1.102	X
VPN IPSEC	500 à 500		X	192.168.1.100	X

Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

8. Le jeu Internet, le serveur ou l'application ne fonctionne pas.

Si vous rencontrez des difficultés pour faire fonctionner correctement un jeu Internet, un serveur ou une application, exposez un ordinateur à Internet à l'aide de l'hébergement DMZ (DeMilitarized Zone). Cette option peut être utilisée lorsqu'une application requiert trop de ports ou lorsque vous ne connaissez pas les services de ports à utiliser. Assurez-vous que toutes les entrées de transfert sont désactivées si vous souhaitez utiliser l'hébergement DMZ. Le transfert a en effet priorité sur l'hébergement DMZ. En d'autres termes, les données qui accèdent à la passerelle seront d'abord contrôlées par les paramètres de transfert. Si le numéro de port à partir duquel les données accèdent n'est pas soumis au transfert de connexion, la passerelle transmet les données à l'ordinateur ou périphérique réseau défini pour l'hébergement DMZ.

- Pour définir l'hébergement DMZ, procédez comme suit :
  1. Accédez à l'utilitaire Web de la passerelle en spécifiant http://192.168.1.1 ou l'adresse IP de la passerelle. Accédez à Applications and Gaming (Applications et jeux) - Onglet DMZ. Cliquez sur Enabled (Activé) et entrez l'adresse IP de l'ordinateur.
  2. Contrôlez les pages Port Forwarding (Transfert de connexion) et désactivez ou supprimez les entrées que vous avez spécifiées pour le transfert. Conservez ces informations au cas où vous souhaiteriez les utiliser ultérieurement.
- Une fois la configuration terminée, cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

9. J'ai oublié mon mot de passe ou l'invite de mot de passe apparaît toujours lorsque j'enregistre des paramètres de la passerelle.

- Réinitialisez les paramètres d'usine de la passerelle. Pour cela, appuyez sur le bouton Reset (Réinitialiser) pendant 10 secondes puis relâchez-le. Si le système continue à vous demander votre mot de passe à l'enregistrement des paramètres, procédez comme suit :
  1. Accédez à l'utilitaire Web de la passerelle en spécifiant http://192.168.1.1 ou l'adresse IP de la passerelle. Entrez le nom d'utilisateur et le mot de passe par défaut **admin** (pour les deux) puis cliquez sur l'onglet **Administrations** (Administrations) => **Management** (Gestion).
  2. Entrez un nouveau mot de passe dans le champ Gateway Password (Mot de passe de la passerelle) et entrez le même mot de passe dans le second champ pour confirmation.
  3. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres).

10. Je souhaite supprimer les paramètres de proxy ou la fenêtre de connexion à distance (pour les utilisateurs PPPoE).

Si vous disposez de paramètres de proxy, vous devez les désactiver sur votre ordinateur. La passerelle étant destinée à la connexion Internet, l'ordinateur n'a pas besoin des paramètres de proxy pour l'accès à Internet. Pour vérifier que vos paramètres de proxy sont supprimés et que le navigateur que vous utilisez est défini pour se connecter directement au réseau local (LAN), procédez comme suit :

- Microsoft Internet Explorer 5.0 ou ultérieur :
  1. Cliquez sur **Démarrer**, **Paramètres** et **Panneau de configuration**. Double-cliquez sur Options Internet.
  2. Cliquez sur l'onglet **Connexions**.
  3. Cliquez sur le bouton **Paramètres réseau** et décochez toutes les cases.
  4. Cliquez sur le bouton **OK** pour revenir à l'écran précédent.
  5. Cochez la case **Ne jamais établir de connexion**. Vous supprimez ainsi toutes les invites de connexion à distance pour les utilisateurs PPPoE.

- Netscape 4.7 ou ultérieur :
  1. Démarrez **Netscape Navigator** et cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**.
  2. Assurez-vous que l'option Connexion directe à Internet est sélectionnée à l'écran.
  3. Fermez toutes les fenêtres pour terminer.

11. Pour recommencer, je dois redéfinir les réglages d'usine de la passerelle.

Appuyez pendant 10 secondes sur le bouton **Reset** (Réinitialiser) puis relâchez-le. Les réglages d'usine sont rétablis pour les paramètres Internet, le mot de passe, le transfert ainsi que tous les autres paramètres. En d'autres termes, la passerelle revient à sa configuration initiale.

12. Je souhaite mettre à niveau le micrologiciel.

Pour mettre à niveau le micrologiciel avec les dernières fonctionnalités, vous devez accéder au site Web international de Linksys à www.linksys.com/international et télécharger le dernier micrologiciel.

- Procédez comme suit :
  1. Accédez au site Web international de Linksys à www.linksys.com/international et sélectionnez votre région ou pays.
  2. Cliquez sur l'onglet **Produit** et sélectionnez la passerelle.
  3. Sur la page Web de la passerelle, cliquez sur **Micrologiciel** puis téléchargez la dernière version disponible.
  4. Pour mettre à niveau la passerelle, suivez les étapes décrites à la rubrique Administration du « Chapitre 5 : Configuration de la passerelle ».

13. La mise à niveau du micrologiciel a échoué et /ou le voyant Power (Alimentation) clignote.

La mise à niveau peut avoir échoué pour diverses raisons. Pour mettre à niveau le micrologiciel et/ou arrêter le clignotement du voyant, procédez comme suit :

- Si la mise à niveau du micrologiciel a échoué, utilisez le programme TFTP (téléchargé avec le micrologiciel). Ouvrez le PDF téléchargé avec le micrologiciel et le programme TFTP et suivez les instructions contenues dans le fichier.
- Définissez une adresse IP statique sur l'ordinateur. Reportez-vous au « Problème 1 : Je souhaite définir une adresse IP statique sur un ordinateur. ». Utilisez les paramètres d'adresse IP suivants pour votre ordinateur :
  Adresse IP : 192.168.1.50
  Masque de sous-réseau : 255.255.255.0
  Passerelle : 192.168.1.1
- Effectuez la mise à niveau à l'aide du programme TFTP ou l'utilitaire Web de la passerelle via l'onglet Administration (Administration).

14. Mon PPPoE de service DSL se déconnecte sans cesse.

PPPoE n'est pas une connexion dédiée ou permanente. Il se peut que le FAI DSL déconnecte le service après une période d'inactivité, comme c'est le cas pour une connexion téléphonique à distance Internet.

- Une option de configuration permet de conserver la connexion « activée ». Il se peut que cela ne fonctionne pas. Dans ce cas, vous devrez rétablir la connexion de temps en temps.

1. Pour connecter la passerelle, ouvrez le navigateur Web et entrez http://192.168.1.1 ou l'adresse IP de la passerelle.
2. Si le système vous y invite, entrez le nom d'utilisateur et le mot de passe. (Par défaut, admin).
3. Sur l'écran Setup (Configuration), sélectionnez l'option **Keep Alive: Redial Period** (Activée : rappel après) et définissez la période à 20 (secondes).
4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres). Cliquez sur l'onglet **Status** (Etat) puis sur le bouton **Connect** (Connecter).
5. Il se peut que l'état de la connexion apparaisse en Connecting (Connexion en cours). Appuyez sur la touche F5 pour actualiser l'affichage jusqu'à ce que son état soit Connected (Connecté).
6. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.

- Si la connexion est de nouveau désactivée, effectuez les étapes 1 à 6 pour la rétablir.

15. Je ne parviens pas à accéder à ma messagerie électronique, au Web ou au VPN, ou je reçois des données corrompues d'Internet.

Il se peut que le paramètre d'unité de transmission maximale (MTU) nécessite une modification. Par défaut, le paramètre MTU est défini automatiquement.

- Si vous rencontrez des difficultés, procédez comme suit :
  1. Pour connecter la passerelle, ouvrez le navigateur Web et entrez http://192.168.1.1 ou l'adresse IP de la passerelle.
  2. Si le système vous y invite, entrez le nom d'utilisateur et le mot de passe. (Par défaut, admin).
  3. Accédez aux options MTU et sélectionnez **Manual** (Manuel). Dans le champ Size (Taille), entrez 1492.
  4. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour continuer.
- Si vous rencontrez toujours des difficultés, essayez différentes valeurs de taille. Essayez la liste de valeurs suivantes (une à la fois et dans cet ordre) jusqu'à ce que le problème soit résolu :
  1462
  1400
  1362
  1300

16. Le voyant Power (Alimentation) d'alimentation clignote.

Le voyant Power (Alimentation) clignote lors de la mise sous tension de l'appareil. Pendant ce temps, le système démarre et vérifie les différents composants. Une fois cette opération terminée, le voyant reste allumé pour indiquer que le système fonctionne correctement. Si le voyant continue à clignoter, le système est défaillant. Essayez de démarrer le micrologiciel en attribuant une adresse IP statique à l'ordinateur, puis mettez à niveau le micrologiciel. Essayez d'utiliser les paramètres suivants. Adresse IP : 192.168.1.50 et Masque de sous-réseau : 255.255.255.0.

17. Lorsque je spécifie une URL ou une adresse IP, j'obtiens une erreur liée à l'expiration du délai et le système m'invite à recommencer.

- Vérifiez si les autres ordinateurs fonctionnent. Si c'est le cas, assurez-vous que les paramètres IP de votre ordinateur sont corrects (adresse IP, masque de sous-réseau, passerelle par défaut et DNS). Redémarrez l'ordinateur défaillant.
- Si l'ordinateur est configuré correctement, mais ne fonctionne toujours pas, vérifiez la passerelle. Assurez-vous qu'elle est branchée et sous tension. Connectez-vous à la passerelle et vérifiez les paramètres. Si vous ne parvenez pas à vous connecter à la passerelle, vérifiez le LAN et les connexions d'alimentation.

- Si la passerelle est configurée correctement, contrôlez votre connexion Internet (modem DSL/câble, etc.). Vous pouvez retirer la passerelle pour vérifier la connexion directe.
- Configurez manuellement les paramètres TCP/IP à l'aide d'une adresse DNS fournie par votre FAI.
- Assurez-vous que le navigateur est configuré pour une connexion directe et que les connexions à distance sont désactivées. Dans Internet Explorer, cliquez sur **Outils**, **Options Internet** puis sur l'onglet **Connexions**. Assurez-vous que la case **Ne jamais établir de connexion** est cochée. Dans Netscape Navigator, cliquez sur **Edition**, **Préférences**, **Avancé** et **Proxies**. Assurez-vous que la case **Connexion directe à Internet** est cochée.

Questions fréquemment posées

Quel est le nombre maximal d'adresses IP que la passerelle peut prendre en charge ?
La passerelle peut prendre en charge jusqu'à 253 adresses IP.

L'intercommunication IPSec est-elle prise en charge par la passerelle ?
Oui, il s'agit d'une fonction intégrée qui est activée par défaut.

Où la passerelle est-elle installée sur le réseau ?
Dans un environnement standard, la passerelle est installée entre la prise murale ADSL et le réseau local (LAN).

La passerelle prend-elle en charge IPX ou AppleTalk ?
Non. TCP/IP est le seul protocole standard pour Internet et est devenu la norme mondiale pour les communications. IPX (protocole de communications NetWare utilisé uniquement pour router des messages d'un nœud à un autre) et AppleTalk (protocole de communications utilisé sur les réseaux Apple et Macintosh) peuvent être utilisés pour les connexions de LAN à LAN, mais ils ne peuvent pas être utilisés entre Internet et un LAN.

La connexion LAN de la passerelle prend-elle en charge Ethernet 100 Mbit/s ?
La passerelle prend en charge 100 Mbit/s par l'intermédiaire d'un commutateur 10/100 Fast Ethernet à détection automatique sur le côté LAN de la passerelle.

Qu'est ce que le NAT (Network Address Translation) et quelle est sa fonction ?
La technologie NAT (Network Address Translation) permet de convertir plusieurs adresses IP d'un réseau local privé en une adresse IP publique sur Internet. Ceci ajoute un niveau de sécurité car l'adresse de l'ordinateur connecté au LAN privé ne transite jamais via Internet. En outre, la technologie NAT permet l'utilisation de la passerelle sur des comptes Internet bon marché alors que l'adresse TCP/IP est fournie par le FAI. L'utilisateur peut posséder plusieurs adresses privées derrière cette adresse unique fournie par le FAI.

La passerelle prend-elle en charge d'autres systèmes d'exploitation que Windows 98SE, Windows Millennium, Windows 2000 ou Windows XP ?
Oui mais Linksys, pour l'instant, ne propose pas de support technique pour l'installation, la configuration et le dépannage de ces systèmes d'exploitation.

La passerelle prend-elle en charge le fichier d'envoi ICQ ?
Oui, à l'aide du correctif suivant : cliquez sur le menu ICQ -> préférence -> onglet Connexions -> et cochez la case indiquant que votre système se trouve derrière un pare-feu ou un proxy. Dans les paramètres du pare-feu, définissez ensuite le délai à 80 secondes. L'utilisateur Internet peut alors envoyer un fichier à un autre utilisateur derrière la passerelle.

Je souhaite définir un serveur Unreal Tournament mais les autres utilisateurs du LAN ne peuvent pas y accéder. Que dois-je faire ?
Si vous avez configuré un serveur Unreal Tournament, vous devez créer une adresse IP statique pour chaque ordinateur du réseau local et transférer les ports 7777, 7778, 7779, 7780, 7781 et 27900 à l'adresse IP du serveur. Vous pouvez également utiliser une étendue de transfert de connexion de 7777 ~ 27900. Si vous souhaitez utiliser UT Server Admin, transférez un autre port. (En règle générale, le port 8080 fonctionne bien, mais il sert à l'administration à distance. Il se peut que vous deviez le désactiver.) Ensuite, dans la section [UWeb.WebServer] du fichier server.ini, définissez ListenPort à 8080 (pour qu'il corresponde au port mappé ci-dessus) et ServerName à l'adresse IP attribuée à la passerelle par votre FAI.

Plusieurs joueurs sur le LAN peuvent-ils accéder à un seul serveur de jeux et jouer simultanément à l'aide d'une seule adresse IP publique ?
Cela dépend du jeu réseau et du type de serveur de jeux que vous utilisez. Par exemple, Unreal Tournament prend en charge les connexions multiples avec une seule adresse IP.

Comment puis-je faire fonctionner Half-Life: Team Fortress avec la passerelle ?
Le port client par défaut pour Half-Life est 27005. « +clientport 2700x » doit être ajouté à la ligne de commande de raccourci HL sur les ordinateurs de votre LAN, x correspondant à 6, 7, 8 et ainsi de suite. Plusieurs ordinateurs peuvent ainsi être connectés au même serveur. Un problème : la version 1.0.1.6 n'autorise pas plusieurs ordinateurs avec la même clé CD à se connecter simultanément, même s'il s'agit du même LAN (ce qui n'est pas le cas avec 1.0.1.3). En matière d'hébergement de jeux, il n'est pas nécessaire que le serveur HL soit dans le DMZ. Transférez uniquement le port 27015 vers l'adresse IP locale du serveur.

La page Web se bloque, les fichiers téléchargés sont corrompus et des caractères illisibles apparaissent à l'écran. Que dois-je faire ?
Forcez votre adaptateur Ethernet à 10 Mbit/s ou en mode semi-duplex, puis désactivez temporairement la fonction « Auto-negotiate » (Auto-négociation) de votre adaptateur Ethernet. (Accédez au Panneau de configuration du réseau dans l'onglet Propriétés avancées de l'adaptateur Ethernet.) Assurez-vous que le paramètre de proxy est désactivé dans le navigateur. Pour plus d'informations, consultez le site Web international de Linksys à l'adresse suivante : www.linksys.com/international.

Si tout le reste échoue au cours de l'installation, que puis-je faire ?
Réinitialisez la passerelle en appuyant sur le bouton Reset (Réinitialiser) jusqu'à ce que le voyant Power (Alimentation) s'éteigne puis s'allume. Réinitialisez votre modem DSL en le mettant hors tension puis sous tension. Téléchargez et installez la dernière version du micrologiciel à partir du site Web international de Linksys, à l'adresse suivante www.linksys.com/international.

Comment serai-je averti de la disponibilité des nouvelles mises à niveau du micrologiciel de la passerelle ?
Toutes les mises à niveau du micrologiciel Linksys sont disponibles sur le site Web international de Linksys à l'adresse www.linksys.com/international. Vous pouvez les télécharger gratuitement. Pour mettre à niveau le micrologiciel de la passerelle, utilisez l'onglet Administration (Administration) de l'utilitaire Web de la passerelle. Si la connexion Internet de la passerelle fonctionne correctement, il est inutile de télécharger une version plus récente du micrologiciel, à moins que cette version ne contienne des nouvelles fonctionnalités que vous souhaitez utiliser.

La passerelle fonctionne-t-elle dans un environnement Macintosh ?
Oui mais les pages de configuration de la passerelle ne sont accessibles que par l'intermédiaire d'Internet Explorer 4.0 ou Netscape Navigator 4.0 (ou version ultérieure) pour Macintosh.

Je ne parviens pas à afficher l'écran de configuration Web de la passerelle. Que puis-je faire ?
Il se peut que vous deviez supprimer les paramètres de proxy sur votre navigateur Internet (par exemple, Netscape Navigator ou Internet Explorer). Consultez la documentation de votre navigateur. Assurez-vous également que votre navigateur est défini pour une connexion directe et que l'option de connexion à distance est désactivée. Dans Internet Explorer, cliquez sur Outils, Options Internet puis sur l'onglet Connexions. Assurez-vous que la case Ne jamais établir de connexion est cochée. Dans Netscape Navigator, cliquez sur Edition, Préférences, Avancé et Proxies. Assurez-vous que la case Connexion directe à Internet est cochée.

Qu'est-ce que l'hébergement DMZ ?
L'hébergement Demilitarized Zone (DMZ) permet à une adresse IP (ordinateur) d'être exposée à Internet. Certaines applications requièrent l'ouverture de plusieurs ports TCP/IP. Il est recommandé de configurer votre ordinateur avec une adresse IP statique si vous souhaitez utiliser l'hébergement DMZ. Pour obtenir une adresse IP LAN, reportez-vous à l'« Annexe D : Recherche des adresses Mac et IP de votre adaptateur Ethernet.

Si l'hébergement DMZ est utilisé, l'utilisateur exposé partage-t-il l'adresse IP publique avec la passerelle ?
Non.

Est-ce que la passerelle transmet les paquets PPTP ou route activement les sessions PPTP ?
La passerelle permet la transmission des paquets PPTP.

La passerelle est-elle compatible avec différentes plates-formes ?
Toutes les plates-formes qui prennent en charge Ethernet et TCP/IP sont compatibles avec la passerelle.

Combien de connexions peuvent être transférées simultanément ?
Théoriquement, la passerelle peut établir 520 sessions simultanément mais vous ne pouvez transférer que 10 étendues du port.

Quelles sont les fonctionnalités avancées de la passerelle ?
Les fonctionnalités avancées de la passerelle sont les paramètres sans fil avancés, les filtres, le transfert de connexion, le routage et DDNS.

Quel est le nombre maximal de sessions VPN que la passerelle peut prendre en charge ?
Ce nombre dépend de plusieurs facteurs. Au moins une session IPSec fonctionne via la passerelle. Néanmoins, des sessions IPSec simultanées sont possibles, en fonction des spécifications de vos VPN.

Comment puis-je savoir si je dispose d'une adresse IP statique ou DHCP ?
Contactez votre FAI pour obtenir cette information.

Comment puis-je faire fonctionner mIRC avec la passerelle ?
Dans l'onglet Port Forwarding (Transfert de connexion), définissez le transfert de connexion à 113 pour l'ordinateur sur lequel vous utilisez mIRC.

La passerelle peut-elle être utilisée en tant que serveur DHCP ?
Oui. Le logiciel serveur DHCP est intégré à la passerelle.

Puis-je exécuter une application à partir d'un ordinateur distant via un réseau sans fil ?
Cela dépend si votre application est conçue ou non pour une utilisation via un réseau. Consultez la documentation de l'application pour déterminer si elle prend en charge le fonctionnement réseau.

Qu'est ce que la norme IEEE 802.11b ?
Il s'agit de l'une des normes IEEE défnie pour les réseaux sans fil. La norme 802.11g permet aux appareils réseau sans fil de différents fabricants de communiquer, si ce matériel est conforme à cette norme 802.11g. Elle définit un taux de transfert de données maximal de 54 Mbit/s et une fréquence de fonctionnement de 2,4 GHz.

Quelles sont les fonctionnalités IEEE 802.11b et IEEE 802.11g prises en charge ?
Le produit prend en charge les fonctions IEEE 802.11b et IEEE 802.11g suivantes :

- Protocole CSMA/CA plus Acknowledge
- Itinérance multi-canaux
- Sélection de débit automatique
- Fonction RTS/CTS
- Fragmentation
- Gestion de l'alimentation

Qu'est ce que le mode Point à point ?
Lorsqu'un réseau sans fil est défini en mode Point à point, les ordinateurs équipés sans fil sont configurés pour communiquer directement entre eux, point à point, sans l'intervention d'un point d'accès.

Qu'est ce que le mode d'infrastructure ?
Lorsqu'un réseau sans fil est défini en mode d'infrastructure, il est configuré pour communiquer avec un réseau via un point d'accès sans fil.

Qu'est-ce que l'itinérance ?
Il s'agit de la capacité d'un utilisateur d'ordinateur portable à communiquer en continu tout en se déplaçant dans une zone supérieure à la zone couverte par un point d'accès unique. Avant d'utiliser la fonction d'itinérance, l'ordinateur doit s'assurer que le numéro de canal est identique au point d'accès de la zone de couverture dédiée.

Pour obtenir une connectivité parfaite sans fil, le LAN sans fil doit incorporer différentes fonctions. Chaque nœud et point d'accès, par exemple, doit toujours accuser réception de chaque message. Chaque nœud doit conserver le contact avec le réseau sans fil même si des données ne sont pas transmises. L'obtention simultanée de ces fonctions requiert une technologie de mise en réseau RF dynamique qui connecte les points d'accès et les nœuds. Dans ce système, le nœud de l'utilisateur final recherche le meilleur accès possible au système. Il évalue tout d'abord les facteurs tels que la longueur et la qualité du signal, le chargement du message par chaque point d'accès et la distance entre chaque point d'accès et la connexion câblée principale. Sur la base de ces informations, le nœud sélectionne ensuite le point d'accès correct et enregistre son adresse. Les communications entre le nœud final et l'ordinateur hôte peuvent être réalisées à partir de la connexion principale et vers la connexion principale.

Lorsque l'utilisateur se déplace, l'émetteur NF du nœud final contrôle régulièrement le système afin de déterminer s'il est en contact avec le point d'accès d'origine ou s'il doit en rechercher un autre. Lorsqu'un nœud ne reçoit plus de confirmation de son point d'accès d'origine, il entreprend une nouvelle recherche. Un fois le nouveau point d'accès trouvé, il l'enregistre et le processus de communication se poursuit.

Qu'est ce que la bande ISM ?

Le FCC et ses homologues internationaux ont défini une largeur de bande destinée à une utilisation hors licence : la bande ISM (Industrial, Scientific and Medical). Le spectre spécifique d'environ 2,4 GHz est disponible dans le monde entier. Il s'agit de la possibilité sans précédent de mettre à disposition des utilisateurs du monde entier un système haut débit sans fil.

Qu'est ce que le Spread Spectrum ?

La technologie Spread Spectrum est une fréquence radio large bande développée par l'armée pour disposer d'un système fiable de transmission des communications sensibles. Elle est conçue pour optimiser l'efficacité de la bande passante pour plus de fiabilité, d'intégrité et de sécurité. En d'autres termes, ce système utilise plus de bande passante que la transmission à faible bande (narrowband). Cependant, l'optimisation produit un signal qui est dans les faits plus important et donc plus facile à détecter, pourvu que le récepteur connaisse les paramètres du signal Spread Spectrum transmis. Si un récepteur n'est pas défini à la bonne fréquence, le signal Spread Spectrum ressemble à un bruit d'arrière-plan. Il existe deux autres possibilités principales : Direct Sequence Spread Spectrum (DSSS) et Frequency Hopping Spread Spectrum (FHSS).

Qu'est-ce que le DSSS ? Qu'est-ce que le FHSS ? Et quelles sont leurs différences ?

FHSS (Frequency-Hopping Spread-Spectrum) utilise un transporteur faible bande (narrowband) qui modifie la fréquence en un modèle connu de l'émetteur et du récepteur. S'il est synchronisé correctement, l'effet net est le maintien d'un canal logique unique. Pour un récepteur non configuré, le signal FHSS ressemble à un bruit d'impulsions courtes. DSSS (Direct-Sequence Spread-Spectrum) génère un modèle de bits redondant pour chaque bit transmis. Ce modèle de bits est appelé une puce (chip ou chipping code). Plus la puce est longue, plus la probabilité est forte d'obtenir les données originales. Même si un ou plusieurs bits de la puce sont endommagés au cours de la transmission, les techniques statistiques intégrées à la radio peuvent restaurer les données originales sans devoir les retransmettre. Pour un récepteur non configuré, DSSS apparaît comme un faible bruit de large bande et est rejeté (ignoré) par la plupart des récepteurs de faible bande (narrowband).

Les informations peuvent-elles être interceptées lors de leur transmission aérienne ?
Le WLAN offre deux types de protections. Au niveau matériel, le WLAN offre une sécurité inhérente de cryptage via la technologie Direct Sequence Spread Spectrum. Au niveau logiciel, le WLAN offre une fonction de cryptage (WEP) qui améliore la sécurité et le contrôle des accès.

Qu'est-ce que le WEP ?
WEP (Wired Equivalent Privacy) est un système de protection des données privées basé sur un algorithme de clé partagée 64 bits ou 128 bits, conforme à la norme IEEE 802.11.

Qu'est ce qu'une adresse MAC ?
L'adresse MAC (Media Access Control) est un numéro unique attribué par le fabricant à un périphérique réseau Ethernet, tel qu'un adaptateur réseau, qui permet au réseau de l'identifier au niveau matériel. Pour des raisons de simplicité d'utilisation, ce numéro est généralement permanent. A la différence des adresses IP, qui peuvent changer dès qu'un ordinateur se connecte au réseau, l'adresse MAC d'un périphérique reste identique, ce qui en fait un identifiant réseau particulièrement fiable.

Comment puis-je réinitialiser la passerelle ?
Appuyez pendant environ 10 secondes sur le bouton Reset (Réinitialiser) situé sur le panneau arrière de la passerelle. Cette opération réinitialise les paramètres d'usine de la passerelle.

Comme puis-je résoudre les problèmes liés à la perte du signal ?
Il n'est pas possible de connaître l'étendue exacte de votre réseau sans fil sans le tester. Chaque obstacle placé entre la passerelle et un ordinateur sans fil crée une perte de signal. Les objets en plomb, le métal, les sols en béton, l'eau et les murs réduisent le signal et son étendue. Placez d'abord la passerelle et l'ordinateur sans fil dans la même pièce et déplacez-là progressivement afin de déterminer l'étendue maximale de votre environnement.

Vous pouvez également essayer d'utiliser différents canaux et éliminer ainsi les interférences liées à un canal spécifique.

Mon signal est excellent mais je ne parviens pas à « voir » mon réseau.
Le WEP est probablement activé sur la passerelle mais désactivé sur votre adaptateur sans fil (ou inversement). Vérifiez que des clés et niveaux WEP (64 ou 128) identiques sont utilisés sur tous les nœuds de votre réseau sans fil.

Combien de canaux/fréquences sont disponibles avec la passerelle ?
Onze canaux sont disponibles, classés de 1 à 11 (en Amérique du nord).

Si certaines de vos questions ne sont pas abordées dans cette annexe reportez-vous au site Web international de Linksys à l'adresse suivante :
www.linksys.com/international.

Annexe B : Sécurité sans fil

Informations importantes relatives aux périphériques sans fil

Linksys souhaite rendre la mise en réseau sans fil aussi fiable et facile que possible. Aussi, gardez à l'esprit les points suivants, lorsque vous installez ou utilisez votre réseau sans fil.

1. Performances

Les performances de votre réseau sans fil dépendent de nombreux facteurs :

Dans un environnement de type Infrastructure, la distance à laquelle vous vous trouvez du point d'accès. Plus vous en serez éloigné, plus la vitesse de transmission sera réduite.

Les interférences liées aux aspects structurels. La forme du bâtiment ou de l'édifice, ainsi que le type et les matériaux de construction peuvent avoir un impact défavorable sur la qualité et la vitesse du signal.

L'emplacement et l'orientation des périphériques sans fil.

2. Interférences

Tout périphérique utilisant le spectre de 2,4 GHz peut engendrer des interférences réseau avec un périphérique sans fil 802.11b ou 802.11g. Exemples de périphériques : téléphones sans fil 2,4 GHz, fours à micro-ondes, lieux publics adjacents et réseaux locaux sans fil 802.11b ou 802.11g voisins.

3. Sécurité

La génération actuelle de produits Linksys intègre plusieurs fonctions de sécurité du réseau que vous devez cependant mettre en oeuvre vous-même.

En voici la liste complète. Il est nécessaire d'appliquer au moins les étapes A à E.

A. Modifiez le SSID par défaut.

B. Désactivez SSID Broadcasts (Diffusion du nom SSID).

C. Modifiez le mot de passe par défaut du compte de l'administrateur.

D. Activez MAC Address Filtering (Filtrage des adresses MAC).

E. Modifiez régulièrement le nom SSID.

F. Activez le cryptage WEP 128 bits. Veuillez noter que ceci réduira les performances de votre réseau.

G. Modifiez les clés de cryptage WEP régulièrement.

Pour plus d'informations sur la mise en oeuvre de ces fonctions de sécurité, reportez-vous au guide de l'utilisateur.

4. Menaces informatiques concernant les réseaux sans fil

Les réseaux sans fil sont faciles à détecter. Les pirates informatiques savent que pour se connecter à un réseau sans fil, les périphériques de mise en réseau sans fil commencent par répondre à des « messages d'incidents ». Ces messages ne sont pas chiffrés et contiennent la plupart des données propres au réseau telles que son SSID (Service Set Identifier) et l'adresse IP de l'ordinateur en réseau ou du point d'accès. Voici la procédure de protection que vous pouvez mettre en place :

Modifiez régulièrement le mot de passe de l'administrateur. Quel que soit le périphérique de mise en réseau sans fil que vous utilisez, n'oubliez pas que les paramètres réseau (nom SSID, clés WEP, etc.) sont enregistrés dans son micrologiciel. Votre administrateur réseau est la seule personne habilitée à modifier les paramètres réseau. Si un pirate informatique vient à connaître le mot de passe de l'administrateur, il a également la possibilité de modifier ces paramètres à sa guise. Aussi, rendez cette information plus difficile à obtenir pour un pirate informatique. Modifiez régulièrement le mot de passe de l'administrateur.

SSID (Nom SSID) Vous devez garder à l'esprit plusieurs informations concernant le nom SSID :

A. Désactivez Broadcast (Diffusion)

B. Faites en sorte que ce nom soit unique

C. Modifiez-le souvent

La plupart des périphériques de mise en réseau sans fil intègrent une option de diffusion du nom SSID. Bien que cette option puisse s'avérer pratique, elle permet à n'importe qui de se connecter à votre réseau sans fil, y compris les pirates informatiques. Par conséquent, ne diffusez pas le nom SSID.

Les périphériques de mise en réseau sans fil possèdent un nom SSID par défaut, configuré en usine (celui de Linksys est « linksys »). Les pirates informatiques connaissent ces noms par défaut et peuvent vérifier s'ils sont utilisés sur votre réseau. Modifiez votre nom SSID, afin qu'il soit unique, tout en évitant d'en choisir un en relation avec votre société ou les périphériques de mise en réseau que vous utilisez.

Modifiez votre nom SSID régulièrement afin que les pirates informatiques qui ont réussi à accéder à votre réseau sans fil se voient contraints de tout recommencer pour retenter d'en forcer l'accès.

Adresse MAC. Activez MAC Address Filtering (Filtrage des adresses MAC). Le filtrage des adresses MAC vous permet de n'autoriser l'accès aux noeuds sans fil qu'à certaines adresses MAC. Le pirate informatique rencontre ainsi plus de difficultés à accéder à votre réseau au moyen d'une adresse MAC choisie au hasard.

Cryptage WEP. Le cryptage WEP (Wired Equivalent Privacy) est souvent considéré comme la panacée en matière de protection sans fil, ce qui n'est pas toujours vrai. Cette technique fournit seulement un niveau de sécurité suffisant pour compliquer la tâche du pirate informatique.

Plusieurs moyens permettent d'optimiser l'efficacité du cryptage WEP :

A. Utilisez le niveau de cryptage le plus élevé.

B. Utilisez une clé partagée.

C. Utilisez plusieurs clés WEP.

D. Modifiez vos clés WEP régulièrement.

La mise en oeuvre du cryptage réduit les performances du réseau. Lors de la transmission de données stratégiques par le biais de votre réseau, vous devez utiliser ce cryptage.

Ces conseils en matière de sécurité vous permettront de préserver votre tranquillité tout en profitant de la technologie la plus pratique et la plus flexible que Linksys vous propose.

Annexe C : Configuration de IPSec entre un ordinateur Windows 2000 ou Windows XP et la passerelle

Introduction

Cette annexe vous explique comment établir un tunnel IPSec sécurisé à l'aide de clés partagées pour connecter un réseau privé via la passerelle VPN et une machine Windows 2000 or XP. Les informations relatives à la configuration d'un serveur Windows 2000 sont disponibles sur le site Web de Microsoft :

Microsoft KB Q252735 - Comment configurer un tunnel IPSec sous Windows 2000 ?
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Bases du dépannage IPSec sous Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

REMARQUE : Notez toutes les modifications que vous effectuez. Ces modifications sont identiques dans l'application Windows « secpol » et l'utilitaire Web du routeur.

Environnement

Les adresses IP et les autres éléments spécifiques aux composants/produits mentionnés dans cette annexe sont des exemples.

REMARQUE : Les instructions et les figures de cette section se rapportent au routeur. Remplacez « Gateway » par « Router ». En outre, le texte à l'écran peut être différent du texte qui apparaît dans les instructions lorsque vous cliquez sur les boutons OK ou Fermer.

Windows 2000 ou Windows XP
Adresse IP : 140.111.1.2 <= Le FAI de l'utilisateur fournit l'adresse IP (exemple uniquement).

Masque de sous-réseau : 255.255.255.0

WAG54G

Adresse IP WAN : 140.111.1.1 <= Le FAI de l'utilisateur fournit l'adresse IP (exemple uniquement).

Masque de sous-réseau : 255.255.255.0
Adresse IP LAN : 192.168.1.1
Masque de sous-réseau : 255.255.255.0

Comment établir un tunnel IPSec sécurisé ?

Etape 1 : Etablissement d'une stratégie IPSec

1. Cliquez sur le bouton **Démarrer**, sélectionnez **Exécuter** et entrez **secpol.msc** dans le champ **Ouvrir**. L'écran *Paramètres de sécurité locaux* s'affiche (figure C-1).

2. Cliquez avec le bouton droit de la souris sur **IP Security Policies on Local Computer** (Stratégies de sécurité IP sur l'ordinateur local) (Win XP) ou sur **Stratégies de sécurité IP sur l'ordinateur local** (Win 2000) et sélectionnez **Créer une stratégie de sécurité IP**.

3. Cliquez sur le bouton **Suivant** puis entrez un nom pour la règle (par exemple, to_Router). puis cliquez sur **Next (Suivant)**.

4. Décochez la case **Activer la règle de réponse par défaut**, puis cliquez sur le bouton **Suivant**.

5. Cliquez sur le bouton **Terminer** en vérifiant que la case **Modifier les propriétés** est cochée.

Figure C-1 : Ecran Paramètres de sécurité locaux

REMARQUE : Les références Windows contenues dans cette section sont des références Windows 2000 et Windows XP. Remplacez les références à « Gateway » par « Router ». En outre, le texte à l'écran peut être différent du texte qui apparaît dans les instructions lorsque vous cliquez sur les boutons OK ou Fermer.

Etape : Création des listes de filtres

Liste de filtres 1 : win->Router

1. Dans ce nouvel écran des propriétés de règles, vérifiez que l'onglet **Règles** est sélectionné (figure C-2). Décochez la case **Utiliser l'Assistant Ajout** puis cliquez sur le bouton **Ajouter** pour créer une nouvelle règle.

2. Assurez-vous que l'onglet **Liste de filtres IP** est sélectionné, puis cliquez sur le bouton **Ajouter** (figure C-3). L'écran *Liste de filtres IP* apparaît (figure C-4). Entrez le nom souhaité pour la liste de filtres (win->Router, par exemple) et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur le bouton **Ajouter**.

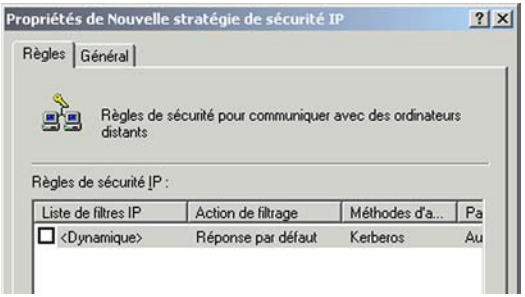

Figure C-2 : Onglet Règles

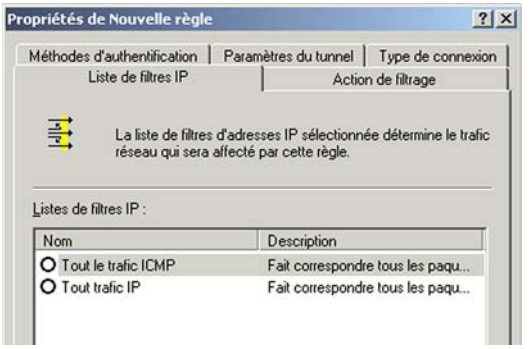
Propriétés de Nouvelle règle
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Liste de filtres IP
Action de filtrage
La liste de filtres d'adresses IP sélectionnée détermine le trafic réseau qui sera affecté par cette règle.
Listes de filtres IP :
Nom
Description
Tout le trafic ICMP
Fait correspondre tous les paqu...
Tout trafic IP
Fait correspondre tous les paqu...

Figure C-3 : Onglet Liste de filtres IP

3. L'écran *Propriétés de Filtrer* apparaît (C-5). Sélectionnez l'onglet **Adressage**. Dans le champ *Adresse source*, sélectionnez **Mon adresse IP**. Dans le champ *Adresse de destination*, sélectionnez **Un sous-réseau IP spécifique** et entrez l'adresse IP : 192.168.1.0 et le masque de sous-réseau : 255.255.255.0. Ce sont les paramètres par défaut du routeur. Si vous avez modifié ces paramètres, entrez les nouvelles valeurs dans ces champs.

4. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet **Description** et saisissez votre description.

5. Cliquez sur le bouton **OK**. Cliquez sur le bouton **OK** ou **Fermer** dans la fenêtre *Liste de filtres IP*.

Liste de filtres 2 : Router=>win

6. L'écran *Propriétés de Nouvelle règle* apparaît (figure C-6). Sélectionnez l'onglet **Liste de filtres IP** et assurez-vous que **win -> router** apparaît en surbrillance. Cliquez ensuite sur le bouton **Ajouter**.

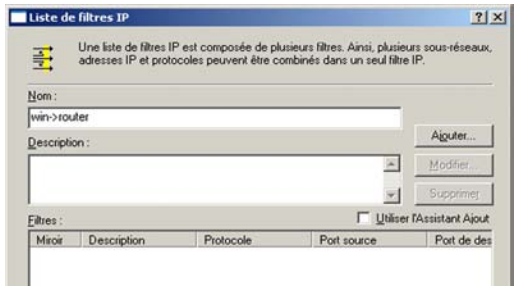

Figure C-4 : Liste de filtres IP

Propriétés de Filtrer
Adressage
Protocole
Description
Adresse source :
Mon adresse IP
Adresse de destination :
Un sous-réseau IP spécifique
Adresse IP :
192 . 168 . 1 . 0
Masque de sous-réseau :
255 . 255 . 255 . 0
Image miroir. Faire coïncider également les paquets possédant des adresses source et de destination exactement opposées.

Figure C-5 : Propriétés de Filtrer

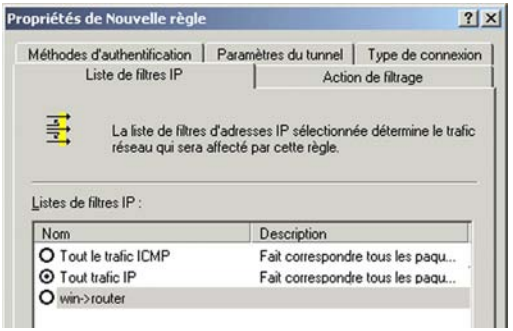
Propriétés de Nouvelle règle
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Liste de filtres IP
Action de filtrage
La liste de filtres d'adresses IP sélectionnée détermine le trafic réseau qui sera affecté par cette règle.
Listes de filtres IP :
Nom
Description
Tout le trafic ICMP
Fait correspondre tous les paqu...
Tout trafic IP
Fait correspondre tous les paqu...
win->router

Figure C-6 : Propriétés de Nouvelle règle

7. L'écran *Liste de filtres IP* apparaît (figure C-7). Entrez le nom souhaité pour la liste de filtres (router->win, par exemple) et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur le bouton **Ajouter**.

8. L'écran *Propriétés de Filtrer* apparaît (figure C-8). Sélectionnez l'onglet Adressage. Dans le champ *Adresse source*, sélectionnez **Un sous-réseau IP spécifique** et entrez l'adresse IP : 192.168.1.0 et le masque de sous-réseau : 255.255.255.0. Si vous avez modifié les paramètres par défaut, entrez vos nouvelles valeurs. Dans le champ Adresse de destination, sélectionnez **Mon adresse IP**.

9. Si vous souhaitez entrer une description de votre filtre, cliquez sur l'onglet *Description* et saisissez votre description.

10. Cliquez sur le bouton **OK** ou le bouton **Fermer**. L'écran *Propriétés de Nouvelle règle* apparaît. L'onglet Liste de filtres IP est sélectionné (figure C-9). « router -> win » et « win -> router » doivent maintenant être répertoriés. Cliquez sur le bouton **OK** (Windows XP) ou **Fermer** (Windows 2000) dans la fenêtre *Liste de filtres IP*.

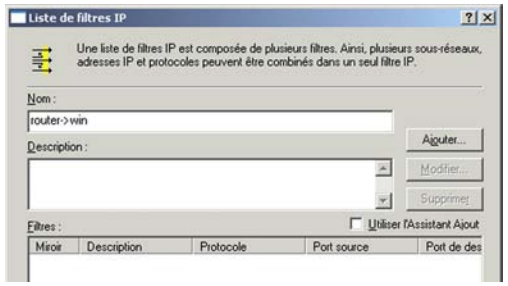

Figure C-7 : Liste de filtres IP

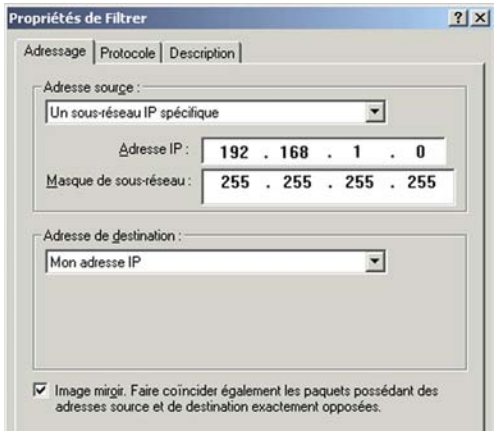
Propriétés de Filtrer
Adressage
Protocole
Description
Adresse source :
Un sous-réseau IP spécifique
Adresse IP :
192 . 168 . 1 . 0
Masque de sous-réseau :
255 . 255 . 255 . 255
Adresse de destination :
Mon adresse IP
Image miroir. Faire coïncider également les paquets possédant des adresses source et de destination exactement opposées.

Figure C-8 : Propriétés de Filtrer

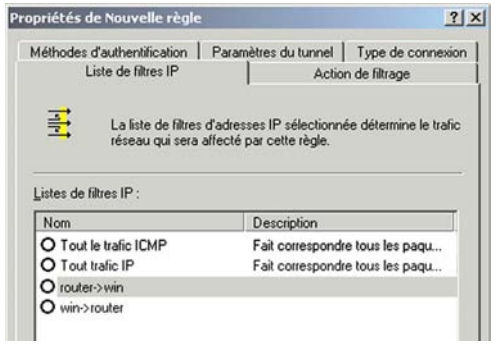

Figure C-9 : Propriétés de Nouvelle règle

Etape 3 : Configuration des règles de tunnel individuelles

Tunnel 1 : win->router

1. Dans l'onglet *Liste de filtres IP* (figure C-10), cliquez sur la liste de filtres win->router.

2. Cliquez sur l'onglet **Action de filtrage** (figure C-11) et cliquez sur le bouton radio **Sécurité requise**. Cliquez ensuite sur le bouton **Modifier**.

3. Dans l'onglet *Méthodes de sécurité* (figure C-12), assurez-vous que l'option **Négocier la sécurité** est activée. Décochez la case **Accepter les communications non sécurisées mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS (Perfect Forward Secrecy)** puis cliquez sur le bouton **OK**.

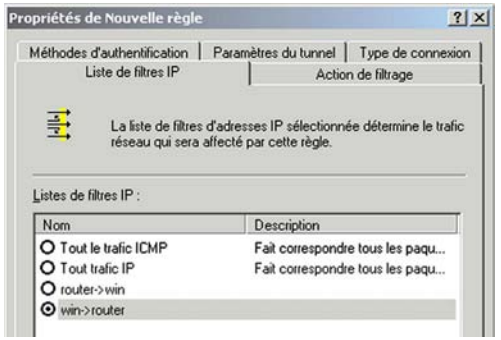

Figure C-10 : Onglet Liste de filtres IP

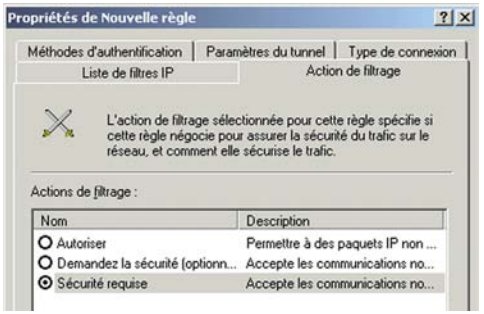
Propriétés de Nouvelle règle
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Liste de filtres IP
Action de filtrage
L'action de filtrage sélectionnée pour cette règle spécifie si cette règle négocie pour assurer la sécurité du trafic sur le réseau, et comment elle sécurise le trafic.
Actions de filtrage :
Nom
Description
Autoriser
Permettre à des paquets IP non ...
Demandez la sécurité (optionn...
Accepte les communications no...
Sécurité requise
Accepte les communications no...

Figure C-11 : Onglet Action de filtrage

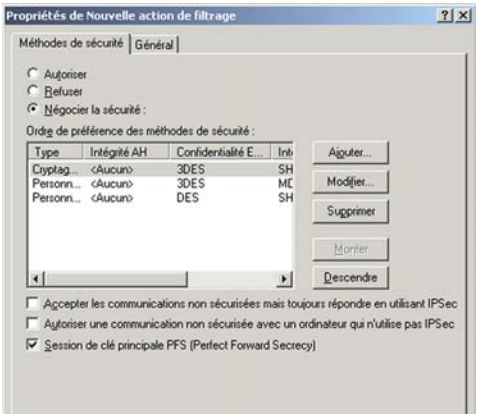

Figure C-12 : Onglet Méthodes de sécurité

4. Sélectionnez l'onglet **Méthodes d'authentification** (figure C-13) puis cliquez sur le bouton **Modifier**.

Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Les méthodes d'authentification définissent les relations d'approbation entre les ordinateurs. Ces méthodes d'authentification sont offertes et acceptées lors de la négociation de la sécurité avec un autre ordinateur.
Ordre de préférence des méthodes d'authentification :
Méthode
Détails
Kerberos
Ajouter...
Modifier...
Supprimer

Figure C-13 : Méthodes d'authentification

5. Sélectionnez la méthode d'authentification **Utiliser cette chaîne (clé partagée au préalable)** (figure C-14) et entrez une chaîne de clé partagée, telle que XYZ12345. Cliquez sur le bouton **OK**.

Propriétés de Éditer la méthode d'authentification
Méthode d'authentification
La méthode d'authentification spécifie la façon dont les relations d'approbation sont établies entre les ordinateurs.
Authentification Active Directory par défaut (protocole Kerberos V5)
Utiliser un certificat émis par cette Autorité de certification :
Parcourir...
Utiliser cette chaîne (clé partagée au préalable) :
XYZ12345

Figure C-14 : Clé pré-partagée

6. Cette nouvelle clé partagée est présentée à la figure C-15. Cliquez sur le bouton **Appliquer** pour continuer (s'il apparaît à l'écran), sinon passez à l'étape suivante.

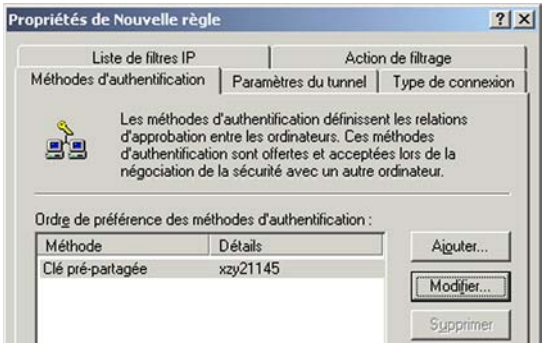
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Les méthodes d'authentification définissent les relations d'approbation entre les ordinateurs. Ces méthodes d'authentification sont offertes et acceptées lors de la négociation de la sécurité avec un autre ordinateur.
Ordre de préférence des méthodes d'authentification :
Méthode
Détails
Clé pré-partagée
xzy21145
Ajouter...
Modifier...
Supprimer

Figure C-15 : Nouvelle clé pré-partagée

7. Sélectionnez l'onglet **Paramètres du tunnel** (figure C-16) et cliquez sur le bouton radio **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Entrez ensuite l'adresse IP WAN du routeur.

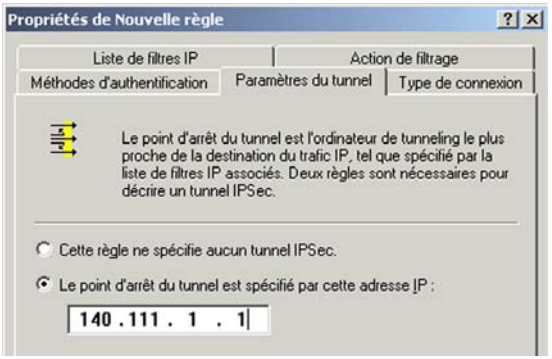
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP associés. Deux règles sont nécessaires pour décrire un tunnel IPSec.
Cette règle ne spécifie aucun tunnel IPSec.
Le point d'arrêt du tunnel est spécifié par cette adresse IP :
140 . 111 . 1 . 1

Figure C-16 : Onglet Paramètres du tunnel

8. Sélectionnez l'onglet **Type de connexion** (figure C-17) et cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** (Windows XP) ou **Fermer** (Windows 2000) pour terminer cette règle.

Tunnel 2 : router->win

9. Dans l'écran Propriétés de Nouvelle stratégie de sécurité IP (figure C-18), assurez-vous que « win -> router » est sélectionné et décochez la case **Utiliser l'Assistant Ajout**. Cliquez ensuite sur **Ajouter** pour créer le second filtre IP.

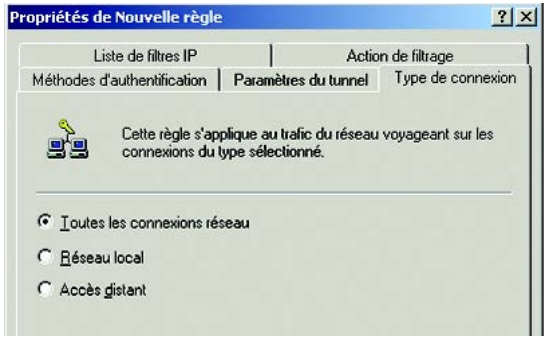
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Cette règle s'applique au trafic du réseau voyageant sur les connexions du type sélectionné.
Toutes les connexions réseau
Réseau local
Accès distant

Figure C-17 : Onglet Type de connexion

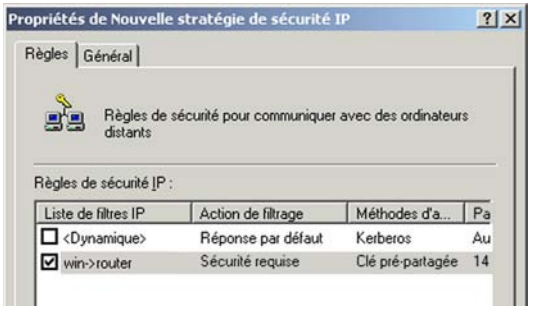

Figure C-18 : Ecran Propriétés de Nouvelle stratégie de sécurité IP

10. Sélectionnez l'onglet **Liste de filtres IP** et cliquez sur la liste de filtres **router->win** (figure C-19).

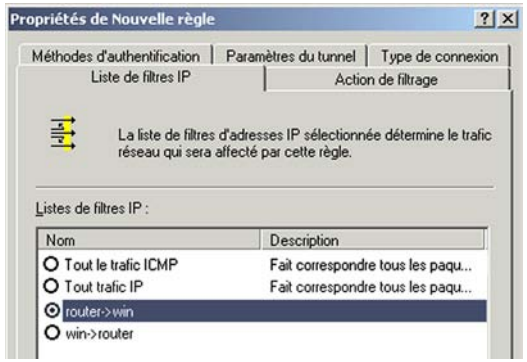

Figure C-19 : Onglet Liste de filtres IP

11. Cliquez sur l'onglet **Action de filtrage** et sélectionnez l'action de filtrage **Sécurité requise** (figure C-20). Cliquez ensuite sur le bouton **Modifier**. Dans l'onglet **Méthodes de sécurité** (figure C-12), assurez-vous que l'option **Négocier la sécurité** est activée. Décochez la case **Accepter les communications non sécurisées mais toujours répondre en utilisant IPSec**. Sélectionnez **Session de clé principale PFS (Perfect Forward Secrecy)** puis cliquez sur le bouton **OK**.

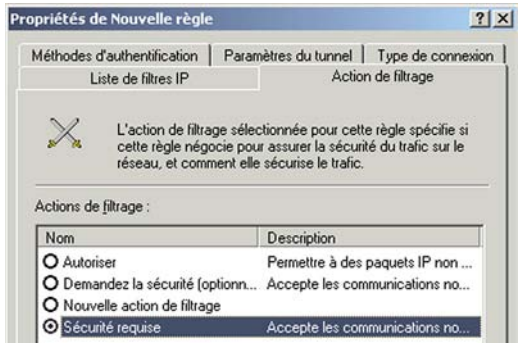
Propriétés de Nouvelle règle
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Liste de filtres IP
Action de filtrage
L'action de filtrage sélectionnée pour cette règle spécifie si cette règle négocie pour assurer la sécurité du trafic sur le réseau, et comment elle sécurise le trafic.
Actions de filtrage :
Nom
Description
Autoriser
Permettre à des paquets IP non ...
Demandez la sécurité (optionn...
Accepte les communications no...
Nouvelle action de filtrage
Sécurité requise
Accepte les communications no...

Figure C-20 : Onglet Action de filtrage

12. Cliquez sur l'onglet **Méthodes d'authentification** et vérifiez que la méthode **Kerberos** est sélectionnée (figure C-21). Cliquez ensuite sur le bouton **Modifier**.

Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Les méthodes d'authentification définissent les relations d'approbation entre les ordinateurs. Ces méthodes d'authentification sont offertes et acceptées lors de la négociation de la sécurité avec un autre ordinateur.
Ordre de préférence des méthodes d'authentification :
Méthode
Détails
Kerberos
Ajouter...
Modifier...

Figure C-21 : Onglet Méthodes d'authentification

13. Sélectionnez la méthode d'authentification **Utiliser cette chaîne (clé partagée au préalable)** (figure C-22) et entrez une chaîne de clé partagée, telle que XYZ12345. Il s'agit d'un exemple de chaîne de clé. Votre clé doit être unique et facile à mémoriser. Cliquez sur le bouton **OK**.

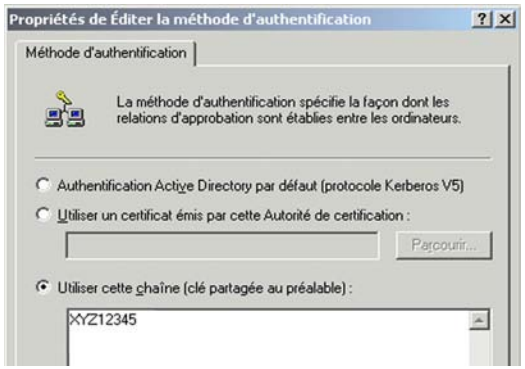
Propriétés de Éditer la méthode d'authentification
Méthode d'authentification
La méthode d'authentification spécifie la façon dont les relations d'approbation sont établies entre les ordinateurs.
Authentification Active Directory par défaut (protocole Kerberos V5)
Utiliser un certificat émis par cette Autorité de certification :
Parcourir...
Utiliser cette chaîne (clé partagée au préalable) :
XYZ12345

Figure C-22 : Clé pré-partagée

14. Cette nouvelle clé pré-partagée est présentée à la figure C-23. Cliquez sur le bouton **Appliquer** pour continuer (s'il apparaît à l'écran), sinon passez à l'étape suivante.

15. Dans l'onglet **Paramètres du tunnel** (figure C-24), cliquez sur le bouton radio **Le point d'arrêt du tunnel est spécifié par cette adresse IP**. Entrez ensuite l'adresse IP de l'ordinateur Windows 2000 ou Windows XP.

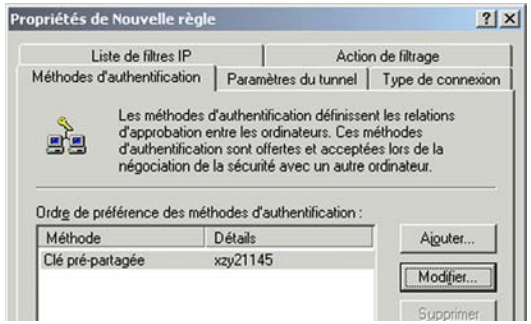
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Les méthodes d'authentification définissent les relations d'approbation entre les ordinateurs. Ces méthodes d'authentification sont offertes et acceptées lors de la négociation de la sécurité avec un autre ordinateur.
Ordre de préférence des méthodes d'authentification :
Méthode
Détails
Clé pré-partagée
xzy21145
Ajouter...
Modifier...
Supprimer

Figure C-23 : Nouvelle clé pré-partagée

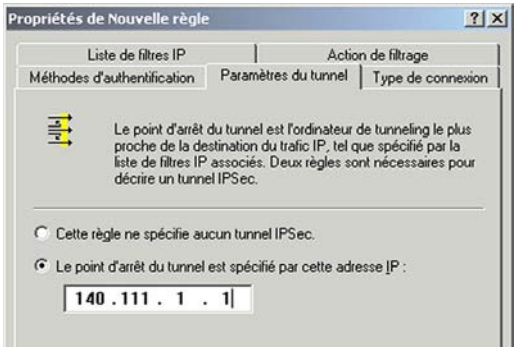
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Le point d'arrêt du tunnel est l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste de filtres IP associés. Deux règles sont nécessaires pour décrire un tunnel IPSec.
Cette règle ne spécifie aucun tunnel IPSec.
Le point d'arrêt du tunnel est spécifié par cette adresse IP :
140 . 111 . 1 . 1

Figure C-24 : Onglet Paramètres du tunnel

16. Sélectionnez l'onglet **Type de connexion** (figure C-25) et cliquez sur **Toutes les connexions réseau**. Cliquez ensuite sur **OK** ou **Fermer** pour terminer cette règle.

17. Dans l'onglet **Règles** (figure C-26), cliquez sur le bouton **OK** ou le bouton **Fermer** pour revenir à l'écran secpol.

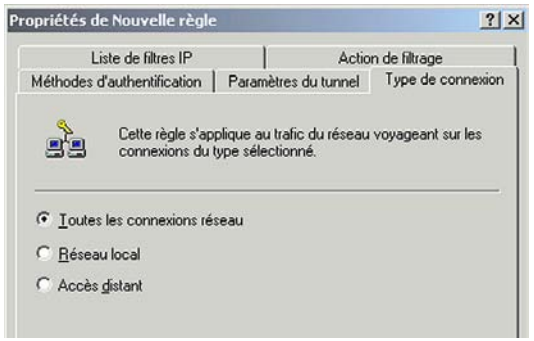
Propriétés de Nouvelle règle
Liste de filtres IP
Action de filtrage
Méthodes d'authentification
Paramètres du tunnel
Type de connexion
Cette règle s'applique au trafic du réseau voyageant sur les connexions du type sélectionné.
Toutes les connexions réseau
Réseau local
Accès distant

Figure C-25 : Type de connexion

Etape 4 : Attribution d'une nouvelle stratégie IPSec

Dans la fenêtre Stratégies de sécurité IP sur Ordinateur local (figure C-27), cliquez à l'aide du bouton droit de la souris sur la stratégie *to_router*, puis cliquez sur **Attribuer**. Une flèche verte apparaît sur l'icône du dossier.

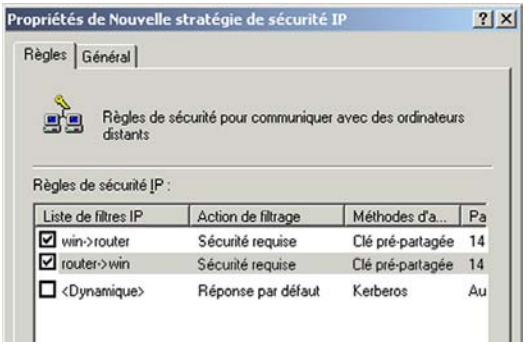

Figure C-26 : Règles

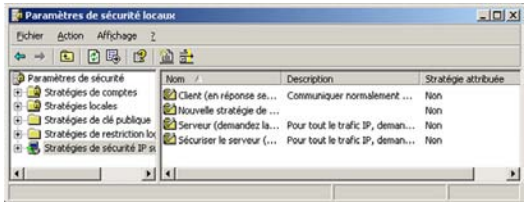

Figure C-27 : Ordinateur local

Etape 5 : Création d'un tunnel à l'aide de l'utilitaire Web

1. Ouvrez votre navigateur Web et entrez **192.168.1.1** dans le champ Adresse. Appuyez sur la touche **Entrée**.
2. Entrez **admin** dans les champs Nom de l'utilisateur et Mot de passe. Appuyez sur la touche **Entrée**.
3. Dans l'onglet *Administration*, cliquez sur l'onglet **VPN**.
4. Dans l'onglet *VPN* (figure C-28), sélectionnez le tunnel que vous souhaitez créer dans la liste déroulante *Select Tunnel Entry* (Sélectionner une entrée de tunnel). Cliquez sur **Enabled** (Activé). Entrez le nom du tunnel dans le champ *Tunnel Name* (Nom du tunnel). Ceci vous permet d'identifier les divers tunnels et il n'est donc pas nécessaire que ce nom corresponde au nom utilisé à l'autre bout du tunnel.
5. Entrez l'adresse IP et le masque de sous-réseau de la passerelle du VPN local dans les champs *Local Secure Group (Groupe sécurisé local)*. Pour autoriser l'accès à l'intégralité du sous-réseau IP, entrez 0 pour le dernier ensemble des adresses IP (par exemple, 192.168.1.0).
6. Entrez l'adresse IP et le masque de sous-réseau du périphérique VPN à l'autre extrémité du tunnel (la passerelle VPN distante ou le périphérique VPN distant avec laquelle/lequel vous voulez communiquer) dans les champs *Remote Security Gateway* (Passerelle de sécurité distante).
7. Sélectionnez l'un des deux types de cryptage : **DES** ou **3DES** (3DES est recommandé car il garantit un niveau de protection plus élevé). Vous pouvez sélectionner l'un de ces deux paramètres, mais le même type de cryptage doit être utilisé par le périphérique VPN à l'autre bout du tunnel. Vous pouvez également ne pas souhaiter utiliser de cryptage. Dans ce cas, sélectionnez l'option **Disable** (Désactiver).
8. Sélectionnez l'un des deux types d'authentification : **MD5** ou **SHA** (SHA est recommandé car il garantit un niveau de protection plus élevé). Comme pour le cryptage, vous pouvez sélectionner l'un de ces deux paramètres, mais le même type d'authentification doit être utilisé par le périphérique VPN à l'autre bout du tunnel. L'authentification peut également être désactivée des deux côtés du tunnel, à l'aide du paramètre **Disable** (Désactiver).
9. Sélectionnez les paramètres de gestion de clé appropriés. Sélectionnez **Auto (IKE)** et saisissez une suite de chiffres ou de lettres dans le champ *Pre-shared Key* (Clé pré-partagée). Cochez la case correspondant à l'option **PFS** (Perfect Forward Secrecy, Secret de transmission total) pour vous assurer que l'échange de clé et les propositions IKE sont sécurisées. Ce champ peut être renseigné à l'aide d'une combinaison de chiffres et de lettres de 24 caractères maximum. Les caractères spéciaux ou les espaces ne sont pas autorisés. Dans le champ *Key Lifetime* (Durée de validité de la clé), vous pouvez sélectionner une date d'expiration de la clé (facultatif). Saisissez la durée de validité de la clé en secondes ou laissez ce champ vierge pour que la clé reste valide indéfiniment.
10. Cliquez sur le bouton **Save Settings** (Enregistrer les paramètres) pour enregistrer les modifications apportées aux paramètres

Votre tunnel est maintenant défini.

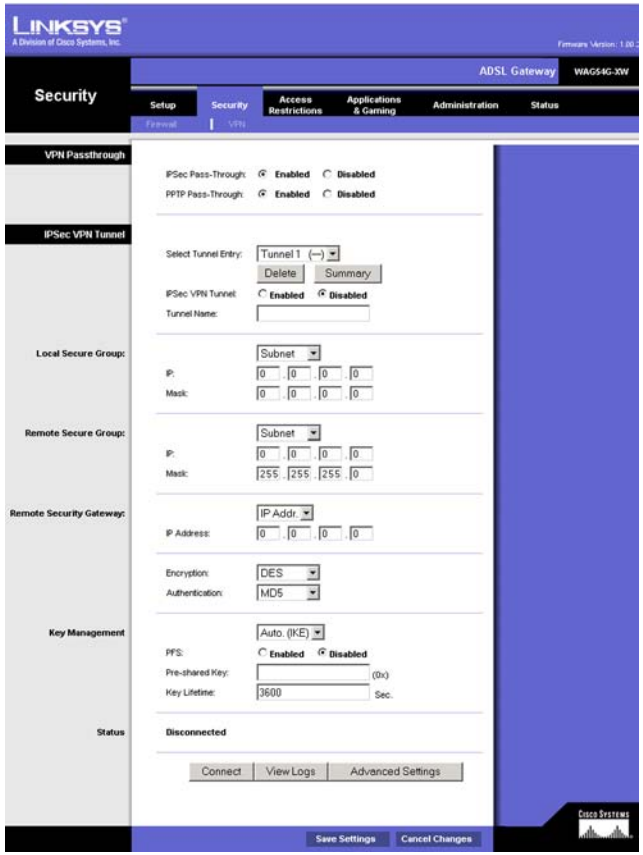

Figure C-28 : Onglet VPN

Annexe D : Recherche des adresses MAC et IP de votre adaptateur Ethernet

Cette section explique comment rechercher l'adresse MAC de l'adaptateur Ethernet de votre ordinateur pour être en mesure d'utiliser la fonctionnalité de filtrage MAC de la passerelle. Vous pouvez également rechercher l'adresse IP de l'adaptateur Ethernet de votre ordinateur. Cette adresse IP est utilisée pour les fonctionnalités de filtrage et/ou DMZ de la passerelle. Veuillez suivre la procédure décrite dans cette annexe pour rechercher l'adresse MAC ou IP de l'adaptateur sous Windows 98, Me, 2000 ou XP.

Instructions pour Windows 98 ou Me

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ *Ouvrir*, saisissez **winipcfg**. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

2. Lorsque l'écran *Configuration IP* apparaît, sélectionnez l'adaptateur Ethernet que vous avez connecté à la passerelle à l'aide d'un câble réseau Ethernet CAT 5 (figure D-1).

3. Notez l'adresse de l'adaptateur qui s'inscrit à l'écran (figure D-2). Il s'agit de l'adresse MAC de votre adaptateur Ethernet. Elle apparaît sous une forme hexadécimale (série de nombres et de lettres).

   L'adresse MAC/adresse de l'adaptateur vous servira pour le filtrage MAC. La figure D-2 présente un exemple d'adresse MAC 00-00-00-00-00-00 pour l'adaptateur Ethernet. Cette adresse sera différente sur votre ordinateur.

   La figure D-2 présente un exemple d'adresse IP 192.168.1.100 pour l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

Remarque : L'adresse MAC est également appelée Adresse de l'adaptateur.

Figure D-1 : Ecran de configuration IP

Figure D-2 : Adresse MAC/Adresse de l'adaptateur

Instructions pour Windows 2000 ou XP

1. Cliquez sur **Démarrer**, puis sélectionnez **Exécuter**. Dans le champ *Ouvrir*, saisissez **cmd**. Appuyez ensuite sur la touche **Entrée** ou cliquez sur **OK**.

Remarque : L'adresse MAC est également appelée Adresse physique.

2. A l'invite de commande, entrez **ipconfig /all**. Appuyez ensuite sur la touche **Entrée**.

3. Notez l'adresse physique indiquée à l'écran (figure D-3). Il s'agit de l'adresse MAC de votre adaptateur Ethernet. Elle apparaît sous une forme hexadécimale (série de nombres et de lettres).

   L'adresse MAC/adresse physique vous servira pour le filtrage MAC. La figure D-3 présente un exemple d'adresse MAC 00-00-00-00-00-00 pour l'adaptateur Ethernet. Cette adresse sera différente sur votre ordinateur.

   La figure E-3 présente un exemple d'adresse IP 192.168.1.100 pour l'adaptateur Ethernet. Cette adresse sera probablement différente sur votre ordinateur.

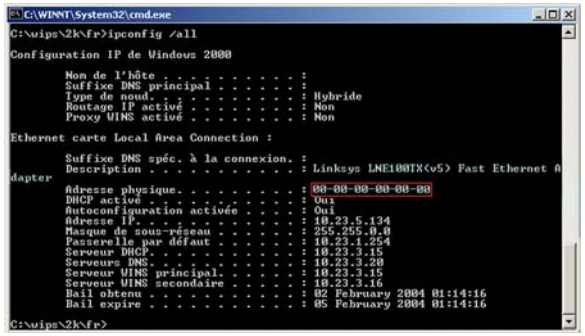
C:\WINNT\System32\cmd.exe
C:\wips\2k\fr>ipconfig /all
Configuration IP de Windows 2000
Nom de l'hôte . . . . . :
Suffixe DNS principal . . . . . :
Type de noud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Ethernet carte Local Area Connection :
Suffixe DNS spéc. à la connexion. :
Description . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
Adresse physique. . . . . : 00-00-00-00-00-00
DHCP activé . . . . . : Oui
Autoconfiguration activée . . . . : Oui
Adresse IP. . . . . : 10.23.5.134
Masque de sous-réseau . . . . . : 255.255.0.0
Passerelle par défaut . . . . . : 10.23.1.254
Serveur DHCP. . . . . : 10.23.3.15
Serveurs DNS. . . . . : 10.23.3.20
Serveur WINS principal. . . . . : 10.23.3.15
Serveur WINS secondaire . . . . . : 10.23.3.16
Bail obtenu . . . . . : 02 February 2004 01:14:16
Bail expire . . . . . : 05 February 2004 01:14:16
C:\wips\2k\fr>

Figure D-3 : Adresse MAC/Adresse Physique

Annexe E : Mise à niveau du micrologiciel

La mise à niveau du micrologiciel de la passerelle s'effectue par l'intermédiaire de l'onglet Upgrade (Mise à niveau) de l'onglet Administration. Procédez comme suit :

1. Cliquez sur le bouton Browse (Parcourir) pour rechercher le fichier de mise à niveau du micrologiciel que vous avez téléchargé à partir du site Web international Linksys puis décompressé. Le micrologiciel disponible sur le site américain ne doit pas être utilisé sur la passerelle.

2. Double-cliquez sur le fichier du micrologiciel que vous venez de télécharger et de décompresser. Cliquez sur le bouton Upgrade (Mettre à niveau) et suivez les instructions à l'écran.

Figure E-1 : Mise à niveau du micrologiciel

Annexe F : Glossaire

802.11a - norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximum de 54 Mbit/s et une fréquence de 5 GHz.

802.11b - norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximum de 11 Mbit/s et une fréquence de 2,4 GHz.

802.11g - norme de mise en réseau sans fil IEEE qui spécifie un débit de transfert de données maximum de 54 Mbit/s, une fréquence de 2,4 GHz et une rétro-compatibilité avec les périphériques 802.11b.

Adaptateur - périphérique ajoutant de nouvelles fonctionnalités réseau à votre ordinateur.

Adresse IP - adresse utilisée pour l'identification d'un ordinateur ou d'un périphérique sur un réseau.

Adresse IP dynamique - adresse IP attribuée provisoirement par un serveur DHCP.

Adresse IP statique - adresse fixe attribuée à un ordinateur ou un périphérique connecté à un réseau.

Adresse MAC (Media Access Control) - adresse unique qu'un fabricant attribue à chaque périphérique d'un réseau.

Bande ISM - bande radio utilisée lors de transmissions réseau sans fil.

Bande passante - capacité de transmission d'un périphérique ou d'un réseau donné.

Base de données - ensemble de données organisées pour faciliter l'accès, la gestion et la mise à jour de leur contenu.

Bit - chiffre binaire.

Commande Finger - programme indiquant le nom associé à une adresse de messagerie.

Commutateur - 1. Périphérique servant de « noyau » de connexion à des ordinateurs ou d'autres périphériques d'un réseau et permettant le partage de données à haut débit. 2. Périphérique permettant de produire, interrompre ou modifier les connexions au sein d'un circuit électrique.

Cryptage - encodage de données pour empêcher qu'elles ne soient lues par des personnes non autorisées.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - méthode de transfert des données adoptée pour éviter la perte de données sur un réseau.

CTS (Clear To Send) - signal émis par un périphérique pour indiquer qu'il est prêt à recevoir des données.

DDNS (Dynamic Domain Name System) - système permettant de disposer d'un site Web, d'un site FTP ou d'un serveur de messagerie avec une adresse IP dynamique et un nom de domaine fixe.

Débit - quantité de données déplacées avec succès d'un noeud à un autre sur une période donnée.

DHCP (Dynamic Host Configuration Protocol) - protocole permettant à un périphérique (appelé serveur DHCP) sur un réseau local d'attribuer des adresses IP temporaires aux périphériques d'un autre réseau, généralement des ordinateurs.

DNS (Domain Name Server) - adresse IP du serveur de votre fournisseur d'accès Internet (FAI). Le système DNS permet de convertir des noms de sites Web en adresses IP.

Domaine - nom spécifique d'un réseau d'ordinateurs.

DSL (Digital Subscriber Line) - connexion haut débit toujours active par le biais des lignes téléphoniques standard.

DSSS (Direct-Sequence Spread-Spectrum) - type de technologie de transmission radio qui introduit un modèle de bit redondant pour diminuer les risques de perte de données lors d'une transmission. Elle est utilisée dans le cadre de réseaux 802.11b.

DTIM (Delivery Traffic Indication Message) - message intégré aux paquets de données et capable d'accroître l'efficacité des structures sans fil.

Etalement du spectre - technique de fréquence radio à large bande utilisée pour une transmission plus fiable et sécurisée des données.

Ethernet - protocole réseau IEEE standard qui spécifie le mode de placement et d'extraction des données via un support de transmission courant.

Expression de passe - utilisée comme un mot de passe, une expression de passe simplifie le processus de cryptage WEP en générant automatiquement les clés de cryptage WEP des produits Linksys.

FAI (fournisseur d'accès Internet) - société offrant un accès à Internet.

Fragmentation - acte de scinder un paquet en unités plus petites lors d'une transmission sur un support réseau inapte à prendre en charge la taille d'origine du paquet.

FTP (File Transfer Protocol) - protocole standard utilisé pour la transmission de fichiers entre des ordinateurs sur un réseau TCP/IP et Internet.

Full Duplex - aptitude d'un périphérique réseau à recevoir et transmettre simultanément des données.

Guirlande - méthode utilisée pour connecter des périphériques en série, l'un après l'autre.

Haut débit - connexion Internet rapide et toujours active.

HTTP (HyperText Transport Protocol) - protocole de communication utilisé pour la connexion à des serveurs sur le World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - institut indépendant chargé du développement des normes réseau standard.

Infrastructure - équipement informatique et réseau actuellement installé.

Initialiser - démarrer un périphérique et lui demander d'exécuter des instructions.

Intervalle de transmission de balise - intervalle de fréquence de la balise, c'est-à-dire un paquet diffusé par une passerelle en vue de synchroniser un réseau sans fil.

IP (Internet Protocol) - protocole utilisé pour transmettre des données sur un réseau.

IPCONFIG - utilitaire des systèmes Windows 2000 et XP qui affiche l'adresse IP d'un périphérique réseau spécifique.

IPSec (Internet Protocol Security) - protocole VPN employé pour la mise en place d'un échange sécurisé des paquets au niveau de la couche IP.

Itinérance - passage d'un périphérique sans fil d'un point d'accès à un autre sans perdre la connexion.

LAN (réseau local) - ordinateurs et produits composant le réseau que vous installez chez vous ou dans vos locaux professionnels.

Logiciel - instructions destinées à l'ordinateur. Série d'instructions destinée à la réalisation d'une tâche donnée appelée « programme ».

Masque de sous-réseau - code d'adresse qui détermine la taille du réseau.

Matériel - présentation physique des ordinateurs, des systèmes de télécommunication et d'autres périphériques liés aux technologies de l'information.

Mbit/s (mégabits par seconde) - un million de bits par seconde ; unité de mesure de transmission des données.

Micrologiciel - 1. Programme destiné à exécuter un périphérique réseau et 2. chargé dans la mémoire morte (ROM) ou la mémoire morte programmable (PROM) que les utilisateurs finaux ne peuvent modifier.

Mise à niveau - acte de remplacer un logiciel ou micrologiciel existant par une nouvelle version.

Mode d'infrastructure - configuration dans laquelle un réseau sans fil est relié à un réseau câblé par l'intermédiaire d'un point d'accès.

Modem câble - périphérique qui relie un ordinateur au réseau de télévision câblé, ce réseau offrant une connexion Internet.

NAT (Network Address Translation) - la technologie NAT permet de convertir les adresses IP d'un réseau local en une adresse IP distincte sur Internet.

Navigateur - application offrant un mode d'affichage et de manipulation des informations sur le World Wide Web.

NNTP (Network News Transfer Protocol) - protocole utilisé pour connecter des groupes Usenet sur Internet.

Nœud - liaison ou point de connexion réseau (généralement, un ordinateur ou une station de travail).

OFDM (Orthogonal Frequency Division Multiplexing) - type de technologie de modulation qui permet de séparer le flux de données en un nombre donné de flux de données à moindre débit, transmis ensuite en parallèle. Cette technologie est utilisée dans le cadre de réseaux 802.11a, 802.11g et PowerLine.

Paquet - unité de données transmises sur un réseau.

Pare-feu - mesures de sécurité protégeant les ressources d'un réseau local contre toute intrusion.

Passerelle - système permettant de relier entre eux des réseaux.

Passerelle par défaut - périphérique utilisé pour transférer un trafic de données Internet depuis votre réseau local.

Ping (Packet INternet Groper) - utilitaire Internet utilisé pour déterminer si une adresse IP particulière est en ligne.

Point à point - groupe de périphériques sans fil communiquant directement entre eux sans l'intervention d'un point d'accès.

Point d'accès - périphérique permettant aux ordinateurs et aux autres périphériques sans fil de communiquer avec un réseau câblé. Il sert également à étendre la portée d'un réseau sans fil.

Pont - périphérique reliant entre eux deux différents types de réseau local (par exemple, un réseau sans fil à un réseau câblé Ethernet).

POP3 (Post Office Protocol 3) - protocole standard utilisé pour extraire des messages électroniques stockés sur un serveur de messagerie.

Port - 1. Port de connexion sur un ordinateur ou un périphérique réseau utilisé pour le branchement à un câble ou un adaptateur. 2. Point de connexion virtuel via lequel un ordinateur exploite une application spécifique sur un serveur.

PPPoE (Point to Point Protocol over Ethernet) - (protocole de point-à-point sur Ethernet) type de connexion haut débit qui permet une authentification (nom d'utilisateur et mot de passe) et le transport des données.

PPTP (Point-to-Point Tunneling Protocol) - (protocole tunnel point-à-point) protocole VPN qui permet au protocole PPP (Point to Point Protocol) de traverser un réseau IP. Il est également utilisé comme type de connexion haut débit en Europe.

Préambule - portion du signal sans fil chargée de synchroniser le trafic réseau.

Réseau - plusieurs ordinateurs ou périphériques reliés entre eux dans le but de partager et de stocker des données et/ou de permettre des transferts entre utilisateurs.

Réseau fédérateur - partie d'un réseau qui permet de relier la plupart des systèmes et des réseaux entre eux et de gérer la majorité des données.

RJ-45 (Registered Jack-45) - connecteur Ethernet pouvant accueillir jusqu'à huit broches.

Routage statique - transfert de données sur un réseau par une voie fixe.

Routeur - périphérique de mise en réseau qui relie entre eux plusieurs ordinateurs (réseau local, Internet).

RTS (Request To Send) - paquet transmis lorsqu'un ordinateur dispose de données qu'il doit transmettre. L'ordinateur attend l'arrivée d'un message CTS (Clear To Send) avant de transmettre les données.

Semi-duplex - transmission de données pouvant survenir dans deux directions sur une ligne unique, mais une direction après l'autre.

Serveur - tout ordinateur dont le rôle sur un réseau est de fournir aux utilisateurs un accès à des fichiers, des imprimantes, des outils de communication et d'autres services.

SMTP (Simple Mail Transfer Protocol) - protocole de messagerie standard utilisé sur Internet.

SNMP (Simple Network Management Protocol) - protocole très répandu de contrôle et d'administration de réseau.

SSID (Service Set IDentifier) - nom de votre réseau sans fil.

Tampon - bloc de mémoire qui stocke provisoirement des données à manipuler ultérieurement lorsqu'un périphérique trop encombré ne peut accueillir ces données.

TCP/IP (Transmission Control Protocol/Internet Protocol) - protocole réseau de transmission de données exigeant la validation de la personne à qui elles sont destinées.

Téléchargement - réception d'un fichier transmis sur un réseau.

Telnet - commande utilisateur et protocole TCP/IP utilisés pour l'accès à des ordinateurs distants.

TFTP (Trivial File Transfer Protocol) - version du protocole FTP TCP/IP qui utilise le protocole UDP et n'offre aucune fonction de répertoire ou de mot de passe.

Topologie - configuration physique d'un réseau.

Transmission multipoint - envoi simultané de données à un groupe de destinataires.

UDP (User Datagram Protocol) - protocole réseau de transmission de données n'exigeant aucune validation de la personne à qui elles sont destinées.

URL (Uniform Resource Locator) - adresse d'un fichier situé sur Internet.

Vitesse de transmission - taux de transmission.

VPN (Virtual Private Network) - mesure de sécurité visant à protéger des données lorsqu'elles quittent un réseau et s'acheminent vers un autre via Internet.

WAN (Wide Area Network) - Internet.

WEP (Wired Equivalent Privacy) - méthode permettant de crypter des données transmises sur un réseau sans fil pour une sécurité accrue.

WINIPCFG - utilitaire Windows 98 et Windows Millennium qui affiche l'adresse IP d'un périphérique réseau spécifique.

WLAN (Wireless Local Area Network) - groupe d'ordinateurs et de périphériques associés qui communiquent entre eux sans fil.

Zone DMZ (zone démilitarisée) - élément qui supprime la protection pare-feu de la passerelle sur un ordinateur et permet ainsi à ce dernier d'être visible sur Internet.

Annexe G : Spécifications

Normes	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), T1.413i2, (Allemagne uniquement : UR-2 Deutsche Telekom)
Ports	Alimentation, LINE (LIGNE) (ADSL), Ethernet (1-4)
Boutons	Un bouton Reset (Réinitialiser), un commutateur On/Off (Marche/Arrêt)
Type de câblage	UTP CAT 5 ou supérieure
Débit de données	Pouvant atteindre 54 Mbit/s (sans fil) Vitesse de téléchargement atteignant 8 Mbit/s (réception) Vitesse de téléchargement atteignant 800 Kbit/s (émission)
Puissance à l'émission	18 dBm
Voyants	Power (Alimentation), Ethernet (1-4), WLAN sans fil G, DSL, Internet
Fonctions de sécurité	Cryptage WEP
Configuration binaire de la clé WEP	64/128 bits
Dimensions (L x H x P)	186 mm x 48 mm x 188 mm (7,32" x 1,89" x 7,40")
Poids	0,48 kg
Alimentation	Externe, 12 Vcc, 1 A

Certifications	FCC Part 15B Class B, FCC Part 15C Class B, FCC Part 68, UL 1950, CSA, CE
Température de fonctionnement	0ºC à 40ºC
Température de stockage	-20ºC à 70ºC
Humidité en fonctionnement	10 à 85 %, non condensée
Humidité de stockage	5 à 90 %, non condensée

Annexe H : Réglementation

DECLARATION FCC

Ce produit a été testé et déclaré conforme aux normes des équipements numériques de catégorie A, conformément à la section 15 des règlements FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie radio fréquence nuisible et s'il n'est pas installé et utilisé selon le manuel d'instruction peut provoquer une interférence nuisible sur les communications radio. Le fonctionnement de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles. Si cet équipement provoque des interférences nuisibles lors de la réception radio ou télévision, détectables en mettant l'équipement hors tension puis sous tension, l'utilisateur peut tenter de remédier à ces interférences en effectuant les opérations suivantes :

- Réorientation ou déplacement de l'antenne de réception
- Augmentation de la distance entre l'équipement ou les périphériques
- Branchement de l'équipement sur une prise autre que celle du récepteur
- Demande d'aide à un revendeur ou un technicien radio/télévision expérimenté

Déclaration FCC sur l'exposition aux radiations
Cet équipement est conforme aux normes FCC en matière d'exposition aux radiations pour un environnement non contrôlé. Cet équipement doit être installé et opérationnel à une distance minimale de 20 cm entre le radiateur et vous-mêmes.

INDUSTRY CANADA (CANADA)

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
Pour pouvoir utiliser cet appareil dans un système fonctionnant partiellement ou complètement en extérieur, l'utilisateur doit obtenir une licence de ce système, en conformité avec la réglementation canadienne.

DECLARATION DE CONFORMITE UE (EUROPE)

Linksys déclare que la passerelle ADSL sans fil G respecte les spécifications énumérées ci-dessous, conformément aux dispositions prévues par la directive européenne R&TTE 1999/5/EC :

- EN 301 489-1, 301 489-17 Spécifications CEM pour les équipements radio.
- Sécurité EN 609 50
- EN 300-328-1, EN 300-328-2 Spécifications techniques pour les équipements radio.

Avertissement : ce matériel a été conçu pour être utilisé dans tous les pays de l'UE et de l'AELE. Son utilisation en extérieur peut faire l'objet de restrictions de fréquences et/ou peut être soumise à autorisation. Vous pouvez contacter les autorités locales pour la procédure à suivre.

Remarque : l'utilisation conjointe de niveaux de puissance et d'antennes générant un niveau de puissance émise supérieur à 100 mW de la puissance isotrope rayonnée équivalente (PIRE) est considérée comme non conforme à la directive susmentionnée et est interdite dans la Communauté Européenne et dans les pays ayant adopté la directive européenne R&TTE 1999/5/EC.

Pour plus de détails sur l'utilisation légale de niveaux de puissance et d'antennes, veuillez contacter le service de conformité aux normes industrielles de Linksys.

- Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

- Linksys Group déclare la Passerelle ADSL sans fil-G conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

- Belgique :

  Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300 m. Pour une distance supérieure à 300 m un enregistrement auprès de l'IBPT est requis. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

- France :

  Bande 2,4 GHz : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complètement libres d'utilisation en France (en intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. L'utilisation en extérieur est soumise à autorisation préalable et très restreinte.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

DECLARATION DE CONFORMITE A L'ARTICLE 68 DES REGLEMENTS FCC

Cet équipement est conforme à la section 68 des règlements FCC (Federal Communications Commission). Vous trouverez sur ce produit une étiquette comportant le numéro d'enregistrement de ce matériel auprès de la FCC ainsi que son numéro REN (Ringer Equivalence Number). Cette information doit être communiquée à la compagnie de téléphone si elle en fait la demande.

Cet équipement utilise la prise USOC suivante : RJ-11

Un cordon téléphonique avec prise jack modulaire conforme aux règlements FCC est livré avec cet équipement. Cet équipement a été conçu pour être connecté au réseau téléphonique ou raccordé au système de câblage d'un bâtiment à l'aide d'une prise jack modulaire compatible, conforme à la section 68 des règlements FCC. La connexion au réseau téléphonique doit être effectuée à l'aide de la prise jack téléphonique modulaire standard.

Le numéro REN (Ringer Equivalence Number) permet de déterminer la quantité d'appareils pouvant être connectés à la ligne téléphonique et permet la sonnerie de tous ces appareils lorsque votre numéro de téléphone est composé. Dans la plupart des zones (mais pas l'intégralité), la somme des REN ne doit pas dépasser 5. Pour être certain du nombre d'appareils pouvant être connectés à une ligne (spécifié par le total des REN), contactez la compagnie de téléphone afin de déterminer le nombre de REN maximal pour votre zone d'appel.

Si cet équipement entraîne une défaillance du réseau téléphonique, la compagnie de téléphone est susceptible de supprimer votre ligne temporairement. Aucun préavis n'est obligatoire. Néanmoins, la compagnie de téléphone notifiera le client dès que possible. En outre, vous serez avisé de vos droits concernant la possibilité de porter plainte auprès de la FCC, si vous jugez cette procédure nécessaire.

La compagnie de téléphone est susceptible de modifier ses équipements, son fonctionnement ou ses procédures, ce qui peut affecter le fonctionnement de votre appareil. Dans ce cas, la compagnie de téléphone vous avertira par avance afin que vous puissiez opérer les modifications nécessaires à la mise en place d'un service ininterrompu.

Si cet équipement ne devait plus fonctionner correctement, déconnectez l'unité de la ligne téléphonique. Essayez de connecter un autre appareil certifié FCC à la même prise téléphonique. Si le problème persiste, contactez le service de dépannage de la compagnie de téléphone. Si le problème est résolu mais que l'unité ne fonctionne pas correctement, déconnectez-la de la ligne téléphonique et ne l'utilisez plus jusqu'à ce qu'elle soit réparée. Veuillez noter que la compagnie de téléphone est susceptible d'exiger le retrait de l'équipement du réseau téléphonique jusqu'à ce que le problème soit résolu ou jusqu'à ce que l'appareil fonctionne de nouveau correctement. L'utilisateur doit utiliser les accessoires et câbles fournis par le fabricant, pour des performances optimales du produit.

Aucune réparation ne doit être effectuée par le client. Si votre équipement ne fonctionne pas correctement, veuillez contacter le service d'assistance technique pour obtenir les informations relatives à la réparation et à la garantie. Si le problème entraîne une défaillance du réseau téléphonique, la compagnie de téléphone est susceptible d'exiger la déconnexion de l'appareil du réseau, jusqu'à ce que le problème soit résolu. Cet équipement ne peut pas être utilisé sur les téléphones à pièces. Le tarif en vigueur pour la connexion à une ligne partagée est celui d'une communication dans l'Etat.

AVERTISSEMENTS RELATIFS A LA SECURITE

- Attention : Afin de réduire les risques d'incendies, utilisez uniquement des câbles téléphoniques No.26 AWG (ou de diamètre supérieur).
- N'utilisez pas le produit à proximité de l'eau, par exemple, sur un sol humide ou près d'une piscine.
- Evitez d'utiliser ces produits (autres que de type sans fil) pendant un orage. Il existe en effet un risque de décharge électrique dû aux éclairs.

Annexe I : Garantie

Responsabilité limitée

Linksys garantit que vos produits Linksys seront, pour l'essentiel, exempts de vices matériels et de fabrication, sous réserve d'une utilisation normale, pendant une période de trois années consécutives (« Période de garantie »). Votre unique recours et l'entière responsabilité de Linksys seront limités, au choix de Linksys, soit à la réparation ou au remplacement du produit, soit au remboursement du prix à l'achat moins les remises effectuées. Cette responsabilité limitée concerne uniquement l'acheteur d'origine.

Si ce produit devait s'avérer défectueux pendant cette période de garantie, contactez le support technique de Linksys pour obtenir, si besoin est, un numéro d'autorisation de retour. N'OUBLIEZ PAS DE CONSERVER VOTRE PREUVE D'ACHAT A PORTEE DE MAIN LORS DE TOUT CONTACT TELEPHONIQUE. Si Linksys vous demande de retourner le produit, indiquez lisiblement le numéro d'autorisation de retour à l'extérieur de l'emballage et joignez-y une copie de l'original de votre preuve d'achat. TOUTE DEMANDE DE RETOUR NE PEUT ETRE TRAITEE EN L'ABSENCE D'UNE PREUVE D'ACHAT. Les frais d'expédition des produits défectueux à Linksys sont à votre charge. Linksys prend uniquement en charge les envois via UPS Ground de Linksys chez Vous. Les frais d'envoi restent à la charge des clients implantés en dehors des Etats-Unis et du Canada.

TOUTES LES GARANTIES IMPLICITES ET CONDITIONS DE VALEUR MARCHANDE OU D'ADEQUATION A UN USAGE PARTICULIER SONT LIMITEES A LA DUREE DE LA PERIODE DE GARANTIE. TOUTES LES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES IMPLICITES OU EXPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE NON CONTREFACON SONT DEMENTIES. Certaines juridictions n'autorisent pas les restrictions relatives à la durée d'une garantie implicite. Par conséquent, la restriction susmentionnée peut ne pas s'appliquer dans votre cas. Cette garantie vous accorde des droits spécifiques. Vous pouvez avoir d'autres droits qui varient en fonction des juridictions.

Cette garantie ne s'applique pas si le produit (a) a été modifié, sauf si cette modification est le fait de Linksys, (b) n'a pas été installé, exploité, réparé ou entretenu conformément aux instructions fournies pas Linksys ou (c) a été altéré suite à une charge physique ou électrique anormale, un usage inadapté du produit, une négligence ou un incident. De plus, en raison du développement permanent de nouvelles techniques visant à infiltrer et attaquer les réseaux, Linksys ne garantit pas que le présent produit est protégé contre toute intrusion ou attaque dont vous feriez l'objet.

CONFORMEMENT A LA LOI ET INDEPENDAMMENT DE LA THEORIE SUR LES RESPONSABILITES, LINKSYS NE POURRA EN AUCUN CAS ETRE TENU RESPONSABLE DES PERTES DE DONNEES, DE REVENUS OU DE BENEFICES OU DES DOMMAGES SPECIAUX, INDIRECTS, CONSECUTIFS, ACCIDENTELS OU DISSUASIFS (Y COMPRIS LES ACTES DE NEGLIGENCE) LIES OU NON LIES A L'UTILISATION OU A L'INCAPACITE A UTILISER LE PRODUIT (Y COMPRIS TOUS LES LOGICIELS), MEME SI LINKSYS A ETE AVERTI DE LA POSSIBILITE DE TELS DOMMAGES. LA RESPONSABILITE DE LINKSYS NE SAURAIT EN AUCUN CAS EXCEDER LE MONTANT QUE VOUS AVEZ EFFECTIVEMENT PAYE POUR L'ACQUISITION DU PRESENT PRODUIT. Les restrictions susmentionnées s'appliqueront même si toutes les garanties ou les recours stipulés dans le présent Contrat ne remplissent pas leur fonction principale. Certaines juridictions n'autorisent pas l'exclusion ou la restriction des dommages accidentels et consécutifs. Par conséquent, la restriction ou l'exclusion susmentionnée peut ne pas s'appliquer dans votre cas.

Cette garantie est valide et peut ne s'appliquer que dans le pays d'acquisition du produit.

Veuillez envoyer toutes vos demandes de renseignement à l'adresse suivante : Linksys, P.O. Box 18558, Irvine, CA 92623.

Annexe J : Contacts

Besoin de contacter Linksys ?
Consultez-nous en ligne pour obtenir des informations sur les derniers produits et les mises à jour disponibles pour vos produits existants à l'adresse suivante :
http://www.linksys.com/international

Si vous rencontrez des problèmes avec un produit Linksys, adressez-nous un courrier électronique et envoyez-le au service Support technique du pays où vous résidez :

Europe	Adresse électronique
Allemagne	support.de@linksys.com
Autriche	support.at@linksys.com
Belgique	support.be@linksys.com
Danemark	support.dk@linksys.com
Espagne	support.es@linksys.com
France	support.fr@linksys.com
Italie	support.it@linksys.com
Norvège	support.no@linksys.com
Pays-Bas	support.nl@linksys.com
Portugal	support.pt@linksys.com
Royaume-Uni et Irlande	support.uk@linksys.com
Suède	support.se@linksys.com
Suisse	support.ch@linksys.com

Hors Europe	Adresse électronique
Amérique Latine	support.la@linksys.com
États-Unis et Canada	support@linksys.com

LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G

ADSL-Gateway Benutzerhandbuch

WIRELESS

Modell-Nr. **WAG54G**

CISCO SYSTEMS

Copyright und Marken

Technische Änderungen vorbehalten. Linksys ist eine eingetragene Marke bzw. eine Marke von Cisco Systems, Inc. und/oder deren Zweigunternehmen in den USA und anderen Ländern. Copyright © 2004 Cisco Systems, Inc. Alle Rechte vorbehalten. Andere Handelsmarken und Produktnamen sind Marken bzw. eingetragene Marken der jeweiligen Inhaber.

Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Gateway ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:

Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.

Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.

Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

Wort: *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

Abbildung 0-1: Kurzbeschreibung der Abbildung

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhalt unter „Abbildungsverzeichnis“.

Inhaltsverzeichnis

Kapitel 1: Einführung 1
- Willkommen 1
- Der Inhalt dieses Handbuchs 2

Kapitel 2: Planen Ihres Netzwerks 4
- Die Funktionen des Gateways 4
- IP-Adressen 4
- Was ist ein VPN? 5
- Wozu benötige ich ein VPN? 6

Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways 8
- Rückseite 8
- Vorderseite 9

Kapitel 4: Anschließen des Wireless-G Broadband-Gateways 10
- Übersicht 10
- Verdrahtete Verbindung mit einem Computer 11
- Wireless-Verbindung mit einem Computer 11

Kapitel 5: Konfigurieren des Gateways 13
- Übersicht 13
- Hinweis für den Zugriff auf das webbasierte Dienstprogramm 15
- Die Registerkarte „Setup“ (Einrichtung) 15
- Die Registerkarte „Wireless“ 23
- Die Registerkarte „Security“ (Sicherheit) 28
- Die Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen) 33
- Die Registerkarte „Applications and Gaming“ (Anwendungen und Spiele) 35
- Die Registerkarte „Administration“ (Verwaltung) 38
- Die Registerkarte „Status“ (Status) 43

Anhang A: Fehlerbehebung 47
- Behebung häufig auftretender Probleme 47
- Häufig gestellte Fragen 55

Anhang B: Sicherheit im Wireless-Netzwerkbetrieb 61
- Wichtige Informationen für drahtlose Produkte 61

Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000/XP-Computer und dem Gateway 64
Einführung 64
Umgebung 64
Hinweise zum Einrichten eines sicheren IPSecTunnels 65
Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters 75
Anweisungen für Windows 98/ME 75
Anweisung für Windows 2000/XP 76
Anhang E: Aktualisieren der Firmware 77
Anhang F: Glossar 78
Anhang G: Spezifikationen 84
Anhang H: Zulassungsinformationen 86
Anhang I: Garantieinformationen 89
Anhang J: Kontaktinformationen 90

Abbildungsverzeichnis

Abbildung 2-1:	Netzwerk	4
Abbildung 2-2:	Computer - VPN-Gateway	6
Abbildung 2-3:	VPN-Gateway - VPN-Gateway	7
Abbildung 3-1:	Rückseite	8
Abbildung 3-2:	Vorderseite	9
Abbildung 4-1:	Ethernet-Verbindung	11
Abbildung 4-2:	ADSL-Verbindung	11
Abbildung 4-3:	Netzstromverbindung	11
Abbildung 5-1:	Fenster zur Kennworteingabe	15
Abbildung 5-2:	Registerkarte „Basic Setup“ (Grundlegende Einrichtung)	15
Abbildung 5-3:	Dynamic IP (Dynamische IP-Adresse)	16
Abbildung 5-4:	Static IP (Statische IP-Adresse)	16
Abbildung 5-5:	RFC 1483 Routed (RFC 1483-Weiterleitung)	17
Abbildung 5-6:	RFC 2516 PPPP over Ethernet	17
Abbildung 5-7:	RFC 2364 PPP over ATM	18
Abbildung 5-8:	Bridged Mode Only (Nur Überbrückungsmodus)	18
Abbildung 5-9:	Optional Settings (Optionale Einstellungen)	19
Abbildung 5-10:	DynDNS.org	20
Abbildung 5-11:	Advanced Routing (Erweitertes Routing)	21
Abbildung 5-12:	Routing Table (Routing-Tabelle)	22
Abbildung 5-13:	Wireless Network Mode (Wireless-Netzwerkmodus)	23
Abbildung 5-14:	WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel)	24
Abbildung 5-15:	WPA RADIUS	24
Abbildung 5-16:	RADIUS	25
Abbildung 5-17:	WEP	25
Abbildung 5-18:	Wireless Network Access (Wireless-Netzwerkzugriff)	26
Abbildung 5-19:	Networked Computers (Netzwerk-Computer)	26
Abbildung 5-20:	Advanced Wireless Settings (Erweiterte Wireless-Einstellungen)	27

Abbildung 5-21:	Firewall	28
Abbildung 5-22:	VPN	29
Abbildung 5-23:	Manual Key Management (Manuelle Schlüsselverwaltung)	30
Abbildung 5-24:	Advanced VPN Tunnel Setup (Erweiterte IPSec VPN-Tunnel-Einrichtung)	31
Abbildung 5-25:	Access Restriction (Zugriffsbeschränkungen)	33
Abbildung 5-26:	Internet Policy Summary (Internet-Richtlinien - Zusammenfassung)	33
Abbildung 5-27:	List of PCs (PC-Liste)	34
Abbildung 5-28:	Port Services (Anschlussdienste)	34
Abbildung 5-29:	Single Port Forwarding (Einfaches Port-Forwarding)	35
Abbildung 5-30:	Port Range Forwarding (Weiterleitung an einen Anschlussbereich)	36
Abbildung 5-31:	Port-Triggering	36
Abbildung 5-32:	DMZ	37
Abbildung 5-33:	Management (Verwaltungsfunktionen)	38
Abbildung 5-34:	Reporting (Berichtaufzeichnung)	40
Abbildung 5-35:	Ping Test (Ping-Test)	41
Abbildung 5-36:	Factory Defaults (Werkseinstellungen)	41
Abbildung 5-37:	Firmware Upgrade (Firmware aktualisieren)	42
Abbildung 5-38:	Status	43
Abbildung 5-39:	Local Network (Lokales Netzwerk)	44
Abbildung 5-40:	DHCP-Client-Tabelle	44
Abbildung 5-41:	Local Network (Wireless-Netzwerk)	45
Abbildung 5-42:	DSL Connection (DSL-Verbindung)	46
Abbildung C-1:	Fenster „Lokale Sicherheitseinstellungen“	65
Abbildung C-2:	Registerkarte „Regeln“	65
Abbildung C-3:	Registerkarte „IP-Filterliste“	65
Abbildung C-4:	Dialogfeld „IP-Filterliste“	66
Abbildung C-5:	Dialogfeld „Eigenschaften von Filter“	66
Abbildung C-6:	Eigenschaften von Neue Regel	66
Abbildung C-7:	Dialogfeld „IP-Filterliste“	67
Abbildung C-8:	Dialogfeld „Eigenschaften von Filter“	67

Abbildung C-9:	Eigenschaften von Neue Regel	67
Abbildung C-10:	Registerkarte „IP-Filterliste“	68
Abbildung C-11:	Registerkarte „Filteraktion“	68
Abbildung C-12:	Registerkarte „Sicherheitsmethoden“	68
Abbildung C-13:	Registerkarte „Authentifizierungsmethoden“	69
Abbildung C-14:	Vorinstallierter Schlüssel	69
Abbildung C-15:	Neuer vorinstallierter Schlüssel	69
Abbildung C-16:	Registerkarte „Tunneleinstellungen“	70
Abbildung C-17:	Registerkarte „Verbindungstyp“	70
Abbildung C-18:	Fenster für die Eigenschaften der neuen Richtlinie	70
Abbildung C-19:	Registerkarte „IP-Filterliste“	71
Abbildung C-20:	Registerkarte „Filteraktion“	71
Abbildung C-21:	Registerkarte „Authentifizierungsmethode“	71
Abbildung C-22:	Vorinstallierter Schlüssel	72
Abbildung C-23:	Neuer vorinstallierter Schlüssel	72
Abbildung C-24:	Registerkarte „Tunneleinstellungen“	72
Abbildung C-25:	Verbindungstyp	73
Abbildung C-26:	Regeln	73
Abbildung C-27:	Lokaler Computer	73
Abbildung C-28:	Registerkarte „VPN“	74
Abbildung D-1:	Fenster „IP-Konfiguration“	75
Abbildung D-2:	MAC-Adresse/Adapteradresse	75
Abbildung D-3:	MAC-Adresse/physikalische Adresse	76
Abbildung E-1:	Firmware aktualisieren	77

Kapitel 1: Einführung

Willkommen

Das Wireless-G ADSL-Gateway von Linksys ist die kompakte Lösung für Internetverbindungen. Die ADSL-Modemfunktion ermöglicht eine extrem schnelle Internetverbindung, die um einiges schneller ist als Einwählverbindungen - ganz ohne Beanspruchen der Telefonleitung.

Schließen Sie Ihre Computer über den integrierten 10/100 Ethernet-Switch mit 4 Ports zum schnellen Hochfahren Ihres Netzwerks an das Gateway an. Sie können Dateien, Drucker, Festplattenspeicher und andere Ressourcen gemeinsam verwenden. Verbinden Sie vier Computer direkt miteinander, oder hängen Sie weitere Hubs und Switches an, um die Größe des Netzwerks Ihren Bedürfnissen gemäß zu gestalten. Der integrierte Wireless-G Access Point (802.11g) ermöglicht den Anschluss von bis zu 32 Wireless-Geräten an Ihr Netzwerk bei einer herausragenden Geschwindigkeit von 54 MBit/s - ganz ohne Kabelverlegung quer durch das Gebäude. Die Kompatibilität mit Wireless-B-Geräten (802.11b) bei einer Geschwindigkeit von 11 MBit/s ist ebenfalls gegeben. Mit der Router-Funktion des Gateways werden all diese Vorteile vereinigt, so dass das gesamte Netzwerk von der High Speed-Internetverbindung profitieren kann.

Zum Schutz Ihrer Daten und Privatsphäre verfügt das Wireless-G ADSL-Gateway über eine erweiterte Firewall, mit der Eindringlinge und Angriffe über das Internet abgewehrt werden. Wireless-Datenübertragungen werden durch leistungsstarke Datenverschlüsselung geschützt. Die Konfiguration ist mit jedem beliebigen Web-Browser kinderleicht.

Mit dem Wireless-G ADSL-Gateway im Zentrum Ihres Netzwerks sind Sie auf dem besten Weg in die Zukunft.

Der Inhalt dieses Handbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Gateways erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Gateways sowie dieses Benutzerhandbuch beschrieben.
- Kapitel 2: Planen Ihres Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.
- Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.
- Kapitel 4: Anschließen des Wireless-G Broadband-Gateways
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an Ihr Netzwerk.
- Kapitel 5: Konfigurieren des Gateways
  In diesem Kapitel wird erläutert, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.
- Anhang A: Fehlerbehebung
  In diesem Anhang werden einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Gateways erörtert.
- Anhang B: Sicherheit im Wireless-Netzwerkbetrieb
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.
- Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000-Computer und dem Gateway
  In diesem Anhang finden Sie Anleitungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden.
- Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Firmware des Gateways, sollte dies einmal erforderlich sein.
- Anhang E: Aktualisieren der Firmware
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.
- Anhang F: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang G: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.
- Anhang H: Zulassungsinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.
- Anhang I: Garantieinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.
- Anhang J: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressoucen, darunter der Kundendienst.

Kapitel 2: Planen Ihres Netzwerks

Die Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway Ihr lokales Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird Ihr Computernetzwerk geschützt, so dass Ihre Computer für andere Benutzer im Internet nicht „sichtbar“ sind. Somit wird der private Charakter Ihres Netzwerks bewahrt. Das Gateway schützt Ihr Netzwerk, indem es alle durch den Internetanschluss eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, falls zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass Sie über die Ports des Gateways eine Verbindung zu zwei verschiedenen Netzwerken herstellen können. Mit den LAN-Ports können Sie eine Verbindung zum LAN und mit dem ADSL-Port eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 MBit/s.

Abbildung 2-1: Netzwerk

***LAN**: Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.*

IP-Adressen

Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein „Standpunkt“ bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, Ihren Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das zugehörige Gerät stets über dieselbe IP-Adresse verfügt, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, wie z. B. Server-Computern oder Druckservern, verwendet.

HINWEIS: Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzerhandbuch wird auf „Internet-IP-Adressen“ und „LAN-IP-Adressen“ verwiesen.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, so dass Gateway und Netzwerk unsichtbar für das Internet sind; weitere Informationen hierzu finden Sie in „Kapitel 5: Konfigurieren des Gateways“ unter „Sicherheit“ in der Beschreibung zum Blockieren von WAN-Anfragen.

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, wie z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als „dynamisch" bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät, wie z. B. das Gateway, fungieren. Standardmäßig ist die DHCP-Serverfunktion des Gateways aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der DHCP-Server deaktivieren. Wenn mehr als ein DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler, wie z. B. IP-Adresskonflikte, auf. Informationen zum Deaktivieren der DHCP-Funktion beim Gateway erhalten Sie in „Kapitel 5: Konfigurieren des Gateways".

Was ist ein VPN?

Ein VPN (*Virtual Private Network*) ist eine Verbindung zwischen zwei Endpunkten (z. B. ein VPN-Gateway) in verschiedenen Netzwerken, mit deren Hilfe private Daten sicher über ein gemeinsam genutztes oder öffentliches Netzwerk, wie z. B. das Internet, gesendet werden können. Dadurch wird ein privates Netzwerk aufgebaut, über das Daten sicher zwischen diesen beiden Standorten bzw. Netzwerken gesendet werden können.

Dies geschieht mithilfe eines „Tunnels". Die beiden Computer oder Netzwerke werden über einen VPN-Tunnel verbunden, durch den Daten über das Internet so übertragen werden können, als ob die Übertragung innerhalb dieser beiden Netzwerke ausgeführt würde. Dabei handelt es sich nicht um einen tatsächlichen Tunnel, sondern um eine Verbindung, die durch die Verschlüsselung der zwischen den Netzwerken gesendeten Daten gesichert wird.

VPN wurde als kostengünstige Alternative zu einer privaten, speziellen, gemieteten Leitung für ein privates Netzwerk entwickelt. Mit Verschlüsselungs- und Authentifizierungstechnologie, die den Industriestandards entspricht (IPSec, Kurzform für *IP Security*, IP-Sicherheit), stellt das VPN eine sichere Verbindung her, die praktisch genauso arbeitet, als ob Sie direkt mit Ihrem lokalen Netzwerk verbunden wären. VPNs können zum Aufbau sicherer Netzwerke verwendet werden, durch die ein Zentralbüro mit Zweigniederlassungen, Telearbeitern und/oder Mitarbeitern im Außendienst verbunden werden kann (Reisende können eine Verbindung zu einem VPN-Gateway von jedem beliebigen Computer mit VPN-Client-Software, die IPSec, wie z. B. SSH Sentinel, unterstützt).

Es gibt zwei grundlegende Möglichkeiten, eine VPN-Verbindung herzustellen:

- VPN-Gateway - VPN-Gateway
- Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Das VPN-Gateway erstellt einen „Tunnel“ bzw. Kanal zwischen zwei Endpunkten, so dass die Datenübertragungen dazwischen sicher sind. Ein Computer mit VPN-Client-Software, die IPSec unterstützt, kann als einer der beiden Endpunkte verwendet werden. Das VPN-Gateway kann von jedem beliebigen Computer mit integriertem IPSec Security Manager (Microsoft 2000 und XP) einen VPN-Tunnel mithilfe von IPSec herstellen (weitere Informationen finden Sie in „Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000/XP-Computer und dem VPN-Gateway“). Für andere Betriebssystemversionen von Microsoft müssen zusätzliche VPN-Client-Softwareanwendungen von Drittanbietern installiert werden, die IPSec unterstützen.

Computer (mit VPN-Client-Software, die IPSec unterstützt) - VPN-Gateway

Im folgenden Beispiel wird ein VPN zwischen einem Computer und einem VPN-Gateway beschrieben (siehe Abb. 2-2). Eine Geschäftsfrau auf Dienstreise stellt in Ihrem Hotelzimmer eine Verbindung mit Ihrem ISP her. Auf ihrem Notebook-Computer ist VPN-Client-Software installiert, die mit den VPN-Einstellungen Ihres Büros konfiguriert ist. Sie ruft die VPN-Client-Software auf, die IPSec unterstützt, und stellt eine Verbindung zum VPN-Gateway im Zentralbüro her. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt die Geschäftsfrau nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob sie physisch damit verbunden wäre.

VPN-Gateway - VPN-Gateway

Ein Beispiel für ein VPN zwischen einem Gateway und einem VPN-Gateway kann folgendermaßen beschrieben werden (siehe Abb. 2-3). Ein Telearbeiter verwendet sein VPN-Gateway zu Hause für seine stets aktive Internetverbindung. Sein Gateway ist mit den VPN-Einstellungen seines Büros konfiguriert. Wenn er eine Verbindung zum Gateway seines Büros herstellt, erstellen die zwei Gateways einen Tunnel, indem Sie die Daten ver- und entschlüsseln. Da VPNs das Internet verwenden, spielt die Entfernung keine Rolle. Über das VPN verfügt der Telearbeiter nun über eine ebenso sichere Verbindung zum Netzwerk des Zentralbüros, als ob er physisch damit verbunden wäre.

Zusätzliche Informationen und Anweisungen zum Erstellen Ihres eigenen VPNs finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international oder in „Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000/XP-Computer und dem VPN-Gateway“.

Wozu benötige ich ein VPN?

Ein Computernetzwerk bietet hochgradige Flexibilität, die bei einem auf Papier basierenden Schriftverkehr nicht gegeben ist. Mit dieser Flexibilität geht jedoch auch ein erhöhtes Sicherheitsrisiko einher. Aus diesem Grund wurden Firewalls entwickelt. Mit Firewalls werden Daten innerhalb eines lokalen Netzwerks geschützt. Aber wie wird dieser Schutz gewährleistet, sobald Informationen an ein Ziel außerhalb Ihres lokalen Netzwerks gesendet werden, wenn E-Mails gesendet werden, oder wenn Sie eine Verbindung zum Netzwerk Ihres Unternehmens herstellen müssen, während Sie unterwegs sind? Wie werden Ihre Daten geschützt?

Abbildung 2-2: Computer - VPN-Gateway

WICHTIG: Sie müssen mindestens ein VPN-Gateway an ein Ende des VPN-Tunnels schalten. Am anderen Ende des VPN-Tunnels muss sich ein anderes VPN-Gateway oder ein Computer mit VPN-Client-Software befinden, die IPSec unterstützt.

Hier kann sich ein VPN als nützlich erweisen. VPNs sichern die Daten, die an ein Ziel außerhalb Ihres Netzwerks gesendet werden, so als ob sie sich immer noch innerhalb des Netzwerks befänden.

Wenn von Ihrem Computer Daten über das Internet gesendet werden, sind sie stets Angriffen ausgesetzt. Möglicherweise verfügen Sie bereits über eine Firewall, mit der die Daten, die verschoben oder an Ziele innerhalb Ihres Netzwerks gesendet werden, vor Angriffen und Beschädigungen von Einheiten außerhalb Ihres Netzwerks geschützt werden. Sobald jedoch Daten an Ziele außerhalb Ihres Netzwerks gesendet werden, d. h. wenn Sie Daten per E-Mail versenden oder mit jemandem über das Internet kommunizieren, werden die Daten nicht mehr durch die Firewall geschützt.

Ihre Daten sind nun Hackern ausgesetzt, die mit einer Reihe von Methoden nicht nur die übertragenen Daten, sondern auch Ihre Netzwerkanmelde- und Sicherheitsdaten stehlen können. Dies sind einige der gängigsten Methoden:

1) MAC-Adressen-Spoofing

Paketen, die über ein Netzwerk, entweder Ihr lokales Netzwerk oder das Internet, übertragen werden, wird eine Paket-Kopfzeile vorangestellt. Diese Paket-Kopfzeilen enthalten sowohl Quell- als auch Zielinformationen, damit das Paket zügig übertragen wird. Ein Hacker kann diese Informationen zum Spoofing (Fälschen) einer auf dem Netzwerk zugelassenen MAC-Adresse verwenden. Mit dieser gefälschten MAC-Adresse kann der Hacker außerdem Informationen für einen anderen Benutzer abfangen.

2) Daten-Sniffing

„Daten-Sniffing“ bezeichnet eine Methode, die von Hackern zum Abrufen von Netzwerkdaten verwendet wird, wenn die Daten sich in unsicheren Netzwerken, wie z. B. dem Internet, befinden. Werkzeuge für diese Aktivitäten, wie z. B. Programme zur Protokollanalyse und Netzwerkdiagnose, sind in vielen Fällen im Betriebssystem integriert und ermöglichen die Anzeige der Daten im Textformat.

3) Man-in-the-Middle-Angriffe

Sobald der Hacker entweder durch Spoofing oder Sniffing genug Informationen gesammelt hat, kann er einen „Man-in-the-Middle-Angriff“ starten. Dieser Angriff wirkt sich so aus, dass Daten, die von einem Netzwerk an ein anderes Netzwerk übertragen werden, an ein neues Ziel umgeleitet werden. Obwohl die Daten von dem vorgesehenen Empfänger nicht empfangen werden, wird dem Absender genau dies angezeigt.

Dies sind nur einige der von Hackern verwendeten Methoden, und es werden stets neue Methoden entwickelt. Ohne die Sicherheit Ihres VPNs sind Ihre Daten ständig solchen Angriffen ausgesetzt, wenn sie über das Internet übertragen werden. Daten, die über das Internet übertragen werden, durchlaufen oftmals viele verschiedene Server in aller Welt, bevor Sie ihr Ziel erreichen. Für nicht geschützte Daten ist dies ein langer Weg; hier erfüllt jedoch ein VPN seinen Zweck.

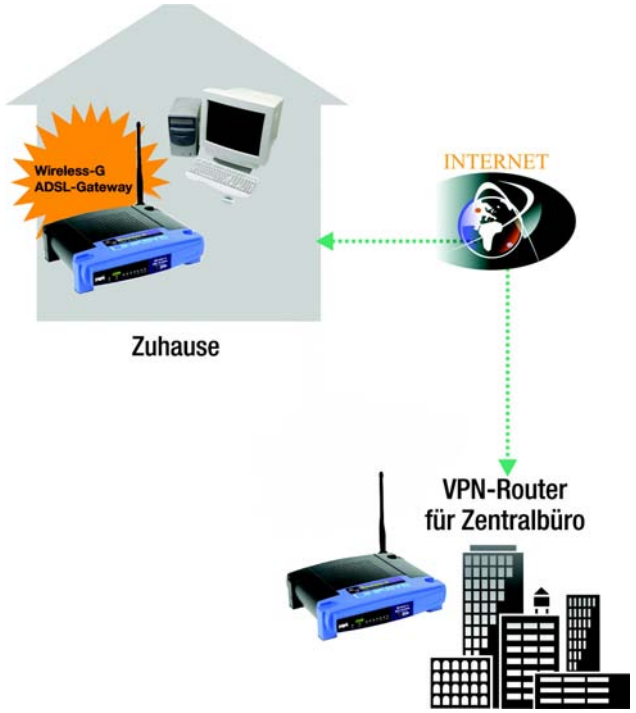

Abbildung 2-3: VPN-Gateway - VPN-Gateway

Kapitel 3: Beschreibung des Wireless-G ADSL-Gateways

Rückseite

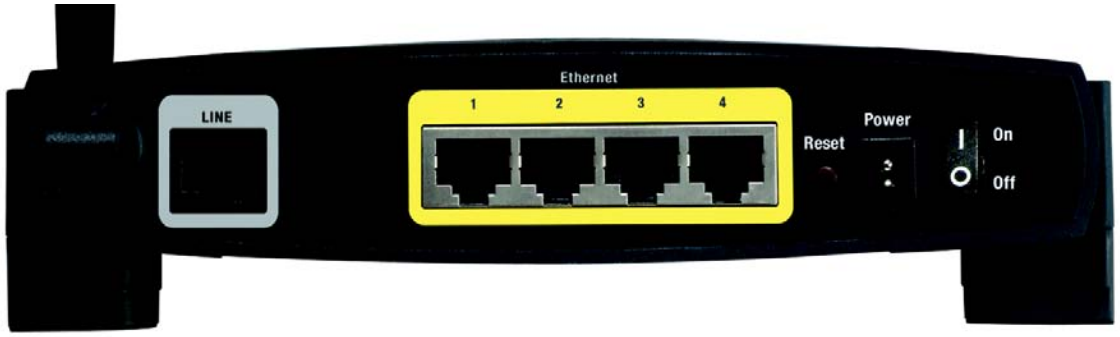

Abbildung 3-1: Rückseite

Die Ports des Gateways für den Anschluss eines Netzwerkkabels befinden sich auf der Rückseite des Geräts. Die Tasten des Gateways befinden sich ebenfalls auf der Rückseite.

LINE (Verbindung) Der **LINE**-Port dient zum Anschließen an die ADSL-Verbindung.

Ethernet (1-4) Die **Ethernet**-Ports dienen zum Anschließen an den Computer und andere Netzwerkgeräte.

Power (Netzstrom) Der Netzstrom-Port dient zum Anschließen des Netzstromadapters.

Reset-Taste Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie entweder die **Reset**-Taste ungefähr zehn Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) unter **Factory Defaults** (Werkseinstellungen) zurück.

On/Off (Ein/Aus) Mit diesem Schalter wird das Gateway ein- und ausgeschaltet.

Mit diesem Produkt, wie mit vielen anderen Linksys Produkten auch, stehen Ihnen grenzenlose Netzwerkbetriebsoptionen offen. Weitere Informationen dazu, welche Produkte mit dem Gateway verwendet werden können, finden Sie auf der internationalen Website von Linksys unter www.linksys.com/international.

Wichtig: Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen (WEP-Verschlüsselung, Wireless- und LAN-Einstellungen usw.) gelöscht und durch die Werkseinstellungen ersetzt. Wenn Sie diese Einstellungen beibehalten möchten, sollten Sie das Gateway nicht zurücksetzen.

Vorderseite

Die LEDs des Gateways, mit denen Informationen zur Netzwerkaktivität angezeigt werden, befinden sich an der Vorderseite.

Abbildung 3-2: Vorderseite

Power (Netzstrom) Grün. Die Netzstrom-LED leuchtet auf, wenn das Gateway eingeschaltet wird.

Ethernet (1-4) Grün. Die **LAN**-LED hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den LAN-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt.

WLAN Grün. Die **WLAN-**LED leuchtet bei jeder erfolgreichen Wireless-Verbindung auf. Wenn die LED blinkt, sendet oder empfängt das Gateway aktiv Daten über das Netzwerk.

DSL Grün. Die **DSL-**LED leuchtet bei jeder erfolgreichen DSL-Verbindung auf. Die LED blinkt, während die ADSL-Verbindung hergestellt wird.

Internet Grün. Die **Internet**-LED leuchtet grün auf, wenn eine Internetverbindung zur Sitzung des Internet-Dienstanbieters (ISP) hergestellt wurde. Die **Internet**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist.

Kapitel 4: Anschließen des Wireless-G Broadband-Gateways

Übersicht

Die Einrichtung des Gateways umfasst mehr als das bloße Anschließen der Hardware. Sie müssen Ihre vernetzten Computer so konfigurieren, dass sie die vom Gateway zugewiesenen IP-Adressen annehmen (falls zutreffend); darüber hinaus müssen Sie das Gateway mithilfe von Einstellungen konfigurieren, die Sie von Ihrem ISP (Internet Service Provider) erhalten.

Sie haben möglicherweise nach der Installation Ihrer Breitbandverbindung die Informationen zur Einrichtung Ihres Modems vom Installationstechniker Ihres ISP erhalten. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und der Einrichtung des Gateways beginnen.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Verdrahtete Verbindung mit einem Computer“ fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Wireless-Verbindung mit einem Computer“ fort.

Verdrahtete Verbindung mit einem Computer

1. Bevor Sie beginnen, stellen Sie sicher, dass all Ihre Hardwaregeräte, einschließlich des Gateways und der Computer, ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1-4 beschriftet) auf der Rückseite des Gateways (siehe Abb. 4-1) und das andere Ende am Ethernet-Port des Computers an.
3. Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.

WICHTIG: Wenn Sie Mikrofilter verwenden, schalten Sie diese nur zwischen das Telefon und die Wandbuchse und nicht zwischen das Gateway und die Wandbuchse. Andernfalls schlägt die ADSL-Verbindung fehl.

4. Schließen Sie ein Ende des Telefonkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an die Wandbuchse der ADSL-Leitung an. Benutzer von Annex A sollten jeweils einen Mikrofilter zwischen Telefon und Wandbuchse verwenden, um Störungen zu vermeiden. Benutzer von Annex B (ADSL über ISDN) sollten ggf. Splitter verwenden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.
5. Schließen Sie den Netzstromadapter an den Stromanschluss des Gateways an (siehe Abb. 4-3), und stecken Sie den Netzstromadapter anschließend in eine Netzsteckdose. Stellen Sie den On-/Off-Schalter auf **On** (Ein).
   - Sobald das Netzgerät richtig angeschlossen und der Schalter auf **On** (Ein) gestellt ist, sollte die Netzstrom-LED auf der Vorderseite grün leuchten. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen ist. Wenn die LED eine Minute oder länger blinkt, finden Sie Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.
6. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

Abbildung 4-1: Ethernet-Verbindung

Abbildung 4-2: ADSL-Verbindung

Wireless-Verbindung mit einem Computer

Befolgen Sie diese Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

1. Bevor Sie beginnen, stellen Sie sicher, dass all Ihre Hardwaregeräte, einschließlich des Gateways und der Computer, ausgeschaltet sind.

HINWEIS: Schließen Sie das Netzgerät des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

Abbildung 4-3: Netzstromverbindung

WICHTIG: Wenn Sie Mikrofilter verwenden, schalten Sie diese nur zwischen das Telefon und die Wandbuchse und nicht zwischen das Gateway und die Wandbuchse. Andernfalls schlägt die ADSL-Verbindung fehl.

2. Schließen Sie ein Ende des Telefonkabels an den LINE-Port auf der Rückseite des Gateways (siehe Abb. 4-2) und das andere Ende an die Wandbuchse der ADSL-Leitung an. Ein sogenannter Mikrofilter muss u. U. zwischen Telefon und Wandbuchse geschaltet werden, um Störungen zu vermeiden. Sollten Sie Fragen hierzu haben, wenden Sie sich an Ihren ISP.
3. Schließen Sie den Netzstromadapter an den Stromanschluss an (siehe Abb. 4-3), und stecken Sie den Netzstromadapter anschließend in eine Netzsteckdose. Stellen Sie den On-/Off-Schalter auf **On** (Ein).
    - Sobald das Netzgerät richtig angeschlossen und der Schalter auf **On** (Ein) gestellt ist, sollte die Netzstrom-LED auf der Vorderseite grün leuchten. Die Netz-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen ist. Wenn die LED eine Minute oder länger blinkt, finden Sie Informationen zur Fehlerbehebung in „Anhang A: Fehlerbehebung“.
4. Schalten Sie einen der Computer in Ihrem Wireless-Netzwerk ein.
5. Stellen Sie für den erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters des Computers auf **linksys** (die Standardeinstellung des Gateways) eingestellt ist und dass die WEP-Verschlüsselung deaktiviert ist. Wenn Sie auf das Gateway zugegriffen haben, können Sie die Einstellungen des Gateways und des Adapters von diesem Computer Ihren üblichen Netzwerkeinstellungen anpassen.

HINWEIS: Sie sollten stets die Standardeinstellung der SSID, **linksys**, ändern und die WEP-Verschlüsselung aktivieren.

Die Installation der Gateway-Hardware ist jetzt abgeschlossen.

Fahren Sie mit „Kapitel 5: Konfigurieren des Gateways“ fort.

Kapitel 5: Konfigurieren des Gateways

Übersicht

Folgen Sie zum Konfigurieren des Gateways den in diesem Kapitel aufgeführten Schritten, und verwenden Sie das webbasierte Dienstprogramm des Gateways. In diesem Kapitel wird jede Webseite des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können über Ihren Web-Browser mithilfe eines an das Gateway angeschlossenen Computers auf das Dienstprogramm zugreifen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie im Fenster **Basic Setup** (Grundlegende Einrichtung) die von Ihrem ISP bereitgestellten Einstellungen ein.
- **Management** (Verwaltungsfunktionen): Klicken Sie auf die Registerkarte **Administration** (Verwaltung) und anschließend auf die Registerkarte **Management** (Verwaltungsfunktionen). Der Standardbenutzername und das Standardkennwort des Gateways lauten **admin**. Ändern Sie das Standardkennwort, um das Gateway zu schützen.

Es stehen sieben Hauptregisterkarten zur Verfügung: **Setup** (Einrichtung), **Wireless** (Wireless), **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen und Spiele), **Administration** (Verwaltung) und **Status** (Status). Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

Haben Sie TCP/IP auf Ihren Computern aktiviert? Computer tauschen über das Netzwerk mit diesem Protokoll Daten aus. Weitere Informationen zu TCP/IP erhalten Sie im Abschnitt „Windows-Hilfe“ in Anhang D.

Hinweis: Für zusätzliche Sicherheit sollten Sie das Kennwort über die Registerkarte **Administration** (Verwaltung) ändern.

Setup (Einrichtung)

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie in dieses Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (Dynamic Domain Name System) des Gateways zu aktivieren.
- **Advanced Routing** (Erweitertes Routing): Sie können in diesem Fenster die Konfigurationseinstellungen für dynamisches und statisches Routing ändern.

Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): Sie können in diesem Fenster den Wireless-Netzwerkmodus und die Wireless-Sicherheitseinstellungen auswählen.
- **Wireless Network Access** (Wireless-Netzwerkzugriff): In diesem Fenster ist die Zugriffsliste für das Wireless-Netzwerk aufgeführt.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Sie können über dieses Fenster auf die erweiterten Wireless-Funktionen zugreifen.

Security (Sicherheit)

- **Firewall**: Dieses Fenster enthält Filter und geblockte WAN-Anfragen. Durch die Verwendung von Filtern kann der Internetzugriff bestimmter interner Benutzer und anonyme Internet-Anfragen geblockt werden.
- **VPN**: Verwenden Sie dieses Fenster, um die Option **IPSec Passthrough** und/oder **PPTP Passthrough** zu aktivieren oder deaktivieren, und richten Sie VPN-Tunnel ein.

Access Restrictions (Zugriffsbeschränkungen)

- **Internet Access** (Internetzugriff): Mithilfe dieses Fensters können Sie bestimmten Benutzern den Zugriff auf Ihr Netzwerk erlauben bzw. deren Zugriff verhindern.

Applications & Gaming (Anwendungen und Spiele)

- **Single Port Forwarding** (Einfaches Port-Forwarding): Verwenden Sie dieses Fenster, um die gängigsten Dienste und Anwendungen auf Ihrem Netzwerk einzurichten.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): Klicken Sie auf diese Registerkarte, um öffentliche Dienste oder weitere spezielle Internet-Anwendungen auf Ihrem Netzwerk einzurichten.
- **Port Triggering** (Port-Triggering): Klicken Sie auf diese Registerkarte, um für Internet-Anwendungen die Bereiche für Port-Triggering und Port-Forwarding festzulegen.
- **DMZ**: Verwenden Sie dieses Fenster, um für einen Benutzer die Internetverbindung zur Verwendung von speziellen Diensten einzurichten.

Administration (Verwaltung)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie Zugriffsrechte für das Gateway sowie SNMP- und UPnP-Einstellungen ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): Verwenden Sie dieses Fenster, um einen Ping-Test durchzuführen.
- **Factory Defaults** (Werkseinstellungen): Verwenden Sie dieses Fenster, wenn Sie das Gateway of die Werkseinstellungen zurücksetzen möchten.
- **Firmware Upgrade** (Aktualisieren der Firmware): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.

Status (Status)

- **Gateway** (Gateway-Adresse): In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des drahtlosen Netzwerks aufgeführt.
- **DSL Connection** (DSL-Verbindung): In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Um auf das webbasierte Dienstprogramm zuzugreifen, starten Sie Internet Explorer oder Netscape Navigator, und geben Sie im Adressenfeld die Standard-IP-Adresse des Gateways (192.168.1.1) ein. Drücken Sie anschließend die Eingabetaste.

Das in Abbildung 5-1 angezeigte Fenster zur Eingabe des Kennworts wird angezeigt. (Unter anderen Betriebssystemen als Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (als Standardbenutzername) in das Feld **Benutzername** sowie **admin** (als Standardkennwort) in das Feld **Kennwort** ein. Klicken Sie dann auf **OK**.

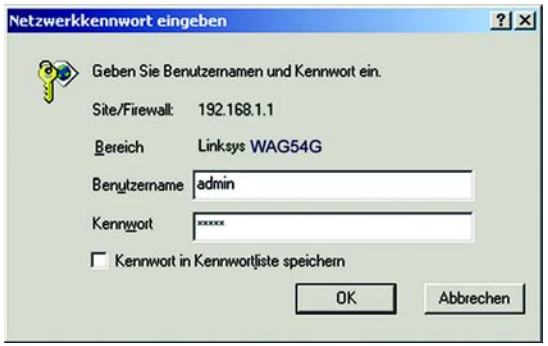

Abbildung 5-1: Fenster zur Kennworteingabe

Die Registerkarte „Setup“ (Einrichtung)

Die Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten dargestellten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt (siehe Abbildung 5-2). Über diese Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Internet Setup (Internet-Einrichtung)

- **VC Settings** (VC-Einstellungen - **Virtual Circuit** Virtueller Kreis): Für diese Option sind zwei Einstellungen erforderlich, **VPI** (*Virtual Path Identifier;* Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier;* Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP. **Multiplexing** (Multiplexing): Wählen Sie entsprechend dem verwendeten ISPs für diese Option **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
- **ADSL Settings** (ADSL-Einstellungen): Das Gateway unterstützt fünf Kapselungstypen: RFC 1483 Bridged, RFC 1483 Routed, RFC 2516 PPPoE, RFC 2364 PPPoA und Bridged Mode Only. Das jeweilige Fenster **Basic Setup** (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.

RFC 1483 Bridged (RFC 1483-Überbrückung)

Dynamic IP (Dynamische IP-Adresse)

IP Settings (IP-Einstellungen): Wählen Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISPs die Verbindung über eine dynamische IP-Adresse herstellen (siehe Abbildung 5-3).

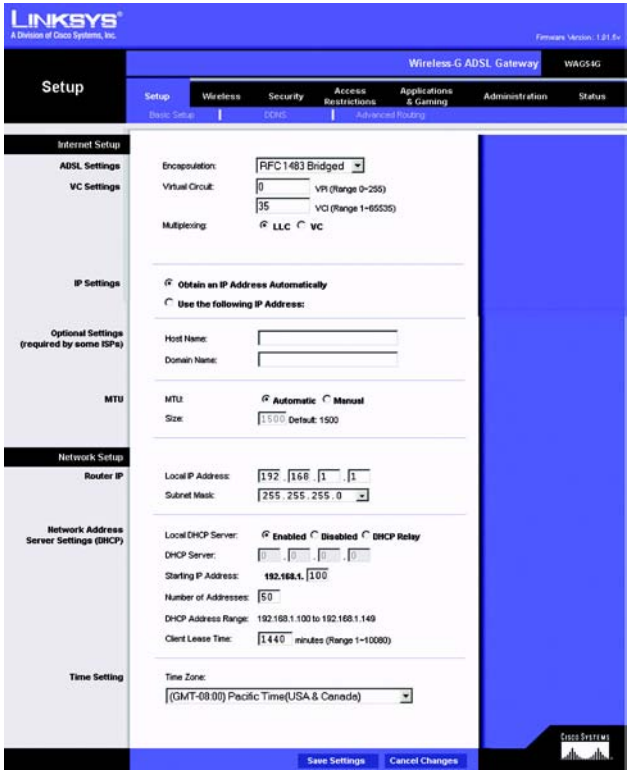

Abbildung 5-2: Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Static IP (Statische IP-Adresse)

Wenn Sie für die Internetverbindung eine permanente IP-Adresse verwenden, wählen Sie **Use the following IP Address** (Folgende IP-Adresse verwenden) aus (siehe Abbildung 5-4).

- **IP Address** (IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die IP-Adresse, die Sie hier angeben müssen, von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS) (erforderliche Einstellung) und **Secondary DNS** (Sekundärer DNS) (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

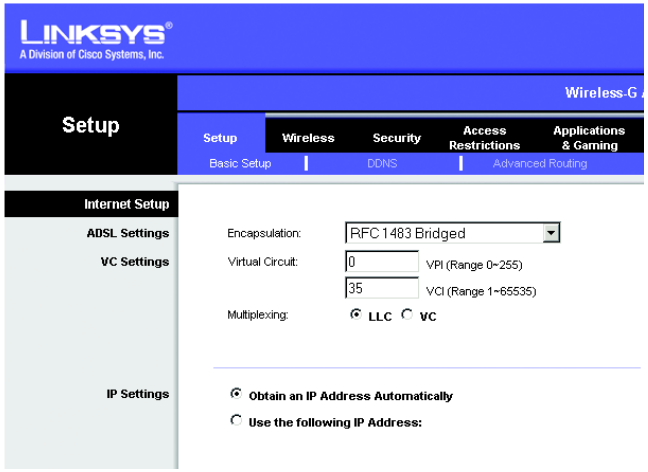

Abbildung 5-3: Dynamic IP (Dynamische IP-Adresse)

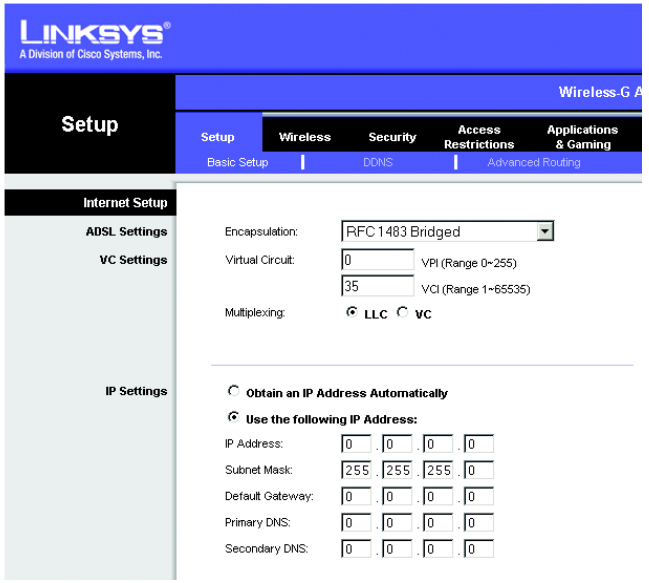

Abbildung 5-4: Static IP (Statische IP-Adresse)

RFC 1483 Routed (RFC 1483-Weiterleitung)

Wählen Sie zur Verwendung des Modus „RFC 1483 Routed“ die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus (siehe Abbildung 5-5).

- **IP Address** (IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die IP-Adresse, die Sie hier angeben müssen, von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Default Gateway** (Standard-Gateway): Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS) (erforderliche Einstellung) und **Secondary DNS** (Sekundärer DNS) (optionale Einstellung): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

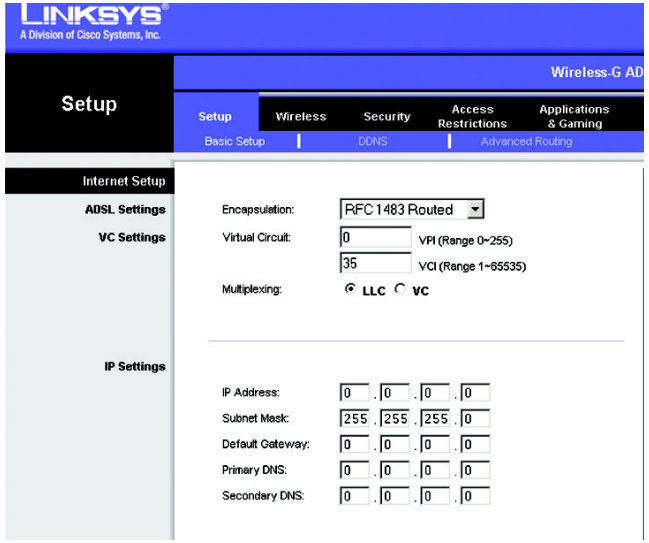

Abbildung 5-5: RFC 1483 Routed (RFC 1483-Weiterleitung)

RFC 2516 PPPoE (RFC 2516 PPP over Ethernet)

Einige ISPs auf DSL-Basis verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoE verwendet wird. Falls ja, wählen Sie die Option **PPPoE** aus (siehe Abbildung 5-6).

- **Service Name** (Dienstname): Geben Sie den Dienstnamen ein, wenn dies für Ihren IP erforderlich ist.
- **User Name** (Benutzername) und **Password** (Kennwort): Geben Sie den Benutzernamen und das Kennwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Connect on Demand** (Bei Bedarf verbinden) zu aktivieren. Geben Sie im Feld **Max Idle Time** (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Klicken Sie zur Verwendung dieser Option auf die Optionsschaltfläche neben **Keep Alive** (Verbindung aufrechterhalten). Im Feld **Redial Period** (Wahlwiederholung) legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

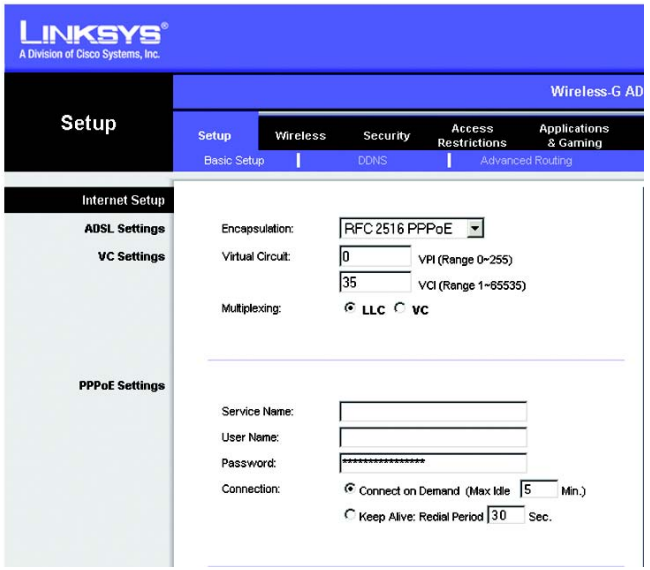

Abbildung 5-6: RFC 2516 PPPP over Ethernet

RFC 2364 PPPoA (RFC 2364 PPP over ATM)

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, wählen Sie die Option **PPPoA** aus (siehe Abbildung 5-7).

- **User Name** (Benutzername) und **Password** (Kennwort): Geben Sie den Benutzernamen und das Kennwort ein, die Sie von Ihrem ISP erhalten haben.
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Klicken Sie auf die entsprechende Optionsschaltfläche, um die Option **Connect on Demand** (Bei Bedarf verbinden) zu aktivieren. Geben Sie im Feld **Max Idle Time** (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Klicken Sie zur Verwendung dieser Option auf die Optionsschaltfläche neben **Keep Alive** (Verbindung aufrechterhalten). Im Feld **Redial Period** (Wahlwiederholung) legen Sie fest, wie oft das Gateway Ihre Internetverbindung überprüfen soll. Die standardmäßige Wahlwiederholung erfolgt nach 30 Sekunden.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

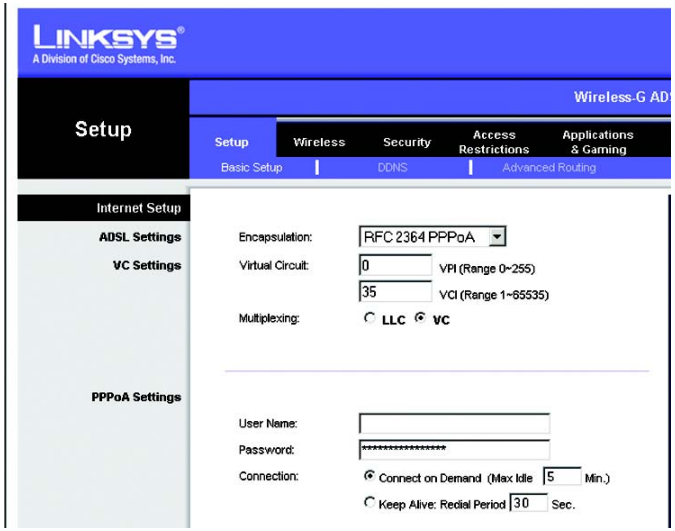

Abbildung 5-7: RFC 2364 PPP over ATM

Bridged Mode Only (Nur Überbrückungsmodus):

Wenn Sie Ihr Gateway als Überbrückung verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Bridged Mode Only** (Nur Überbrückungsmodus) aus (siehe Abbildung 5-8). In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

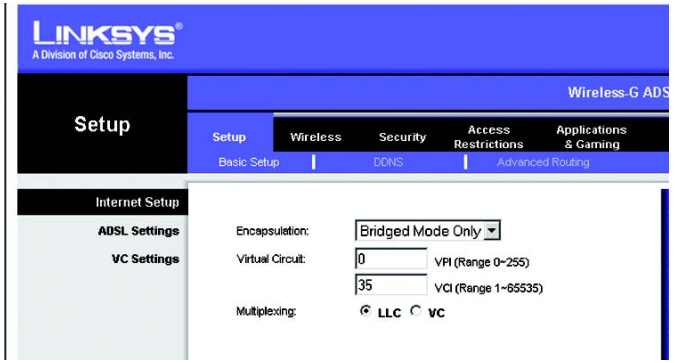

Abbildung 5-8: Bridged Mode Only (Nur Überbrückungsmodus)

Optional Settings (Required by some ISPs) (Zusätzliche Einstellungen, für einige ISPs erforderlich) (siehe Abbildung 5-9)

- **Host Name/Domain Name** (Hostname/Domänenname): In diese Felder können Sie einen Hostnamen bzw. Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Wenden Sie sich an Ihren ISP, um zu ermitteln, ob Ihr Broadband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU:** Durch die MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie die Option **Manual** (Manuell) aus, und geben Sie den gewünschten Wert ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

Network Setup (Netzwerkeinrichtung)

- **Router IP** (IP-Adresse des Routers): Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
  - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist 192.168.1.1.
  - **Subnet Mask** (Subnetzmaske): Der Standardwert ist 255.255.255.0.
- **Network Address Server Settings (DHCP)** [Einstellungen des Netzwerkadressenservers (DHCP)]: Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen.
  - **Local DHCP Server** (Lokaler DHCP-Server): Die DHCP-Option ist standardmäßig aktiviert. Wenn auf Ihrem Netzwerk bereits ein DHCP-Server vorhanden ist, legen Sie für die DHCP-Option des Gateways **Disable** (Deaktivieren) fest.
  - **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.12 betragen, da die Standard-IP-Adresse für das Gateway 192.168.1.1 ist.
  - **Number of Address** (Adressenanzahl): Geben Sie die maximale Anzahl der PCs ein, denen der DHCP-Server IP-Adressen zuweisen soll. Diese Zahl darf nicht größer als 253 sein. Der Standardbereich liegt zwischen 192.168.1.100 und 192.168.1.149 (siehe Abbildung 5-9).
  - **DHCP Address Range** (DHCP-Adressenbereich): Der Bereich der DHCP-Adressen ist hier aufgeführt.
  - **Client Lease Time** (Client-Leasedauer): Geben Sie in dieses Feld die Minutenanzahl ein.
- **Time Setting** (Zeiteinstellung): Mit dieser Option legen Sie die Zeitzone für Ihr Gateway fest.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

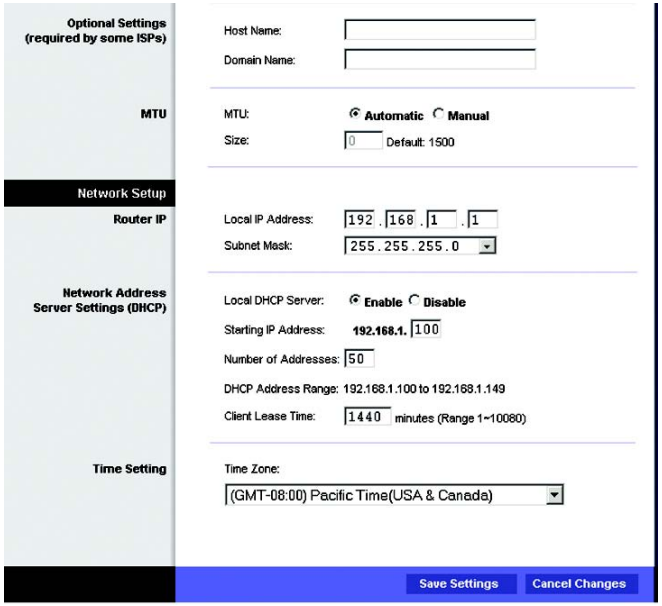

Abbildung 5-9: Optional Settings (Optionale Einstellungen)

Die Registerkarte „DDNS“

Das Gateway verfügt über die Funktion **DDNS** (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich bei den DDNS-Dienstanbietern unter www.dyndns.org anmelden.

DDNS

DDNS Service (DDNS-Dienst): Wenn der von Ihnen verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie im Dropdown-Menü die Option **DynDNS.org** aus (siehe Abbildung 5-10). Um den DDNS-Dienst zu deaktivieren, wählen Sie die Option **Disabled** (Deaktivieren) aus.

DynDNS.org

- **User Name** (Benutzername), **Password** (Kennwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Kennwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet IP Address** (Internet-IP-Adresse): Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Der Status der Verbindung zum DDNS-Dienst ist hier aufgeführt.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Abbildung 5-10: DynDNS.org

Die Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster **Advanced Routing** (Erweitertes Routing) können Sie die Einstellungen für dynamisches und statisches Routing konfigurieren (siehe Abbildung 5-11).

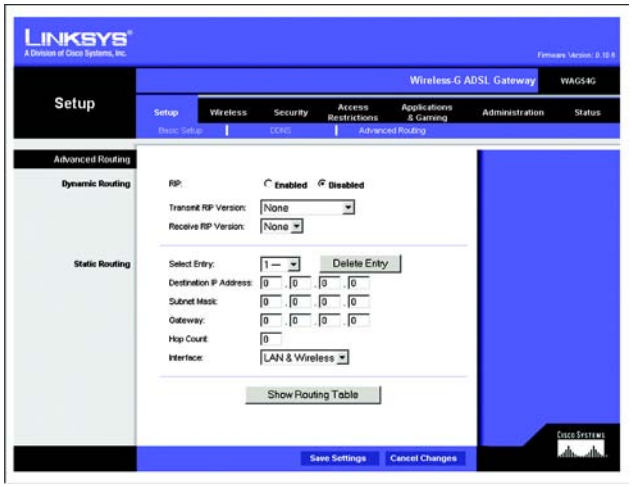

Abbildung 5-11: Advanced Routing (Erweitertes Routing)

Advanced Routing (Erweitertes Routing):

- **Dynamic Routing** (Dynamisches Routing): Mithilfe der Option **Dynamic Routing** (Dynamisches Routing) kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Das Gateway legt unter Verwendung des RIP-Protokolls die Route der Netzwerkpakete auf der Grundlage der geringsten Anzahl an Sprüngen zwischen Quelle und Ziel fest. Das RIP-Protokoll sendet in regelmäßigen Abständen Routing-Information an andere Gateways im Netzwerk. Klicken Sie zum Aktivieren des RIP-Protokolls auf **Enabled** (Aktiviert). Klicken Sie zum Deaktivieren des RIP-Protokolls auf **Disabled** (Deaktiviert).
- **Receive RIP Version** (RIP-Version empfangen): Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**. Wenn Sie keine RIP-Nachrichten empfangen möchten, wählen Sie **None** (Keine).
- **Transmit RIP Version** (RIP-Version übertragen): Wählen Sie zum Übertragen von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1, RIP1-Compatible** (RIP1-kompatibel) oder **RIP2**. Wenn Sie keine RIP-Nachrichten übertragen möchten, wählen Sie **None** (Keine).

Static Routing (Statisches Routing)

Wenn das Gateway an mehr als einem Netzwerk angeschlossen ist, muss u. U. zwischen den Gateways eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:

- **Select Entry** (Eintrag auswählen): Wählen Sie die Anzahl der statischen Routen aus dem Dropdown-Menü aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routeneinträge. Wenn Sie nach Auswahl eines Eintrags eine Route löschen möchten, klicken Sie auf die Schaltfläche **Delete Entry** (Eintrag löschen).
- **Destination IP Address** (Ziel-IP-Adresse): Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert 0 festgelegt ist.
- **Subnet Mask** (Subnetzmaske): Mithilfe der Subnetzmaske (auch Netzwerkmaske genannt) wird festgelegt, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.
- **Gateway** (Gateway-Adresse): Bei dieser IP-Adresse handelt es sich um die IP-Adresse des Gateway-Geräts, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.
- **Hop Count** (Routeranzahl): Hiermit wird die maximale Anzahl von Schritten zwischen den Netzwerkknoten festgelegt, die die Datenpakete passieren. Ein Knoten ist jeder Router im Pfad zum entfernten Netzwerk.

- **Interface** (Schnittstelle): Wählen Sie hierfür die Option **LAN**, **Wireless** oder **Internet** entsprechend der Position des Endziels der statischen Route aus.
- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um dadurch ein Fenster anzuzeigen, in dem die durch ihr LAN übertragenen Daten aufgeführt sind (siehe Abbildung 5-12). Für jede Route wird die Ziel-IP-Adresse, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

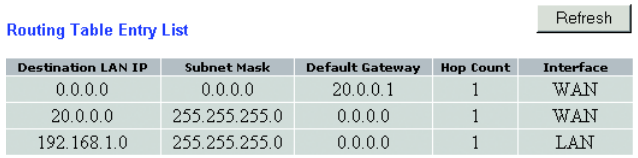

Abbildung 5-12: Routing Table (Routing-Tabelle)

Die Registerkarte „Wireless“

Die Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)
(siehe Abbildung 5-13)

Mithilfe dieses Fensters können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.

Wireless Network (Wireless-Netzwerk)

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn ausschließlich 802.11g-Geräte vorhanden sind, wählen Sie **802.11g** aus. Wenn ausschließlich 802.11b-Geräte vorhanden sind, wählen Sie **802.11b** aus. Um das drahtlose Netzwerk zu deaktivieren, wählen Sie **Disable** (Deaktivieren).
- **Wireless Network Name (SSID)** [Wireless-Netzwerk-Name (SSID)]: Geben Sie in dieses Feld den Namen für Ihr Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerk-Namen, der von allen Geräten im drahtlosen Netzwerk verwendet wird. Die SSID muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird in Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.
- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Hierbei handelt es sich um einen Wert zwischen 1 und 11 (für Nordamerika). Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Clients von Linksys erkennen automatisch den Wireless-Kanal des Gateways.
- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Clients im lokalen Netzwerk nach einer Verbindung zu Wireless-Netzwerken suchen, erkennen sie die Übertragung der SSID über den Router. Zur Übertragung der SSID des Routers behalten Sie die Standardeinstellung **Enabled** (Aktiviert) bei. Wenn Sie die SSID des Routers nicht übertragen möchten, wählen Sie **Disabled** (Deaktiviert) aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

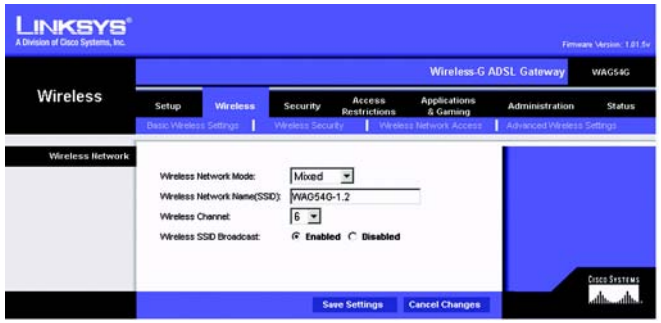

Abbildung 5-13: Wireless Network Mode (Wireless-Netzwerkmodus)

Die Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit Ihres Wireless-Netzwerks konfiguriert. Vom Router werden vier Wireless-Sicherheitsoptionen unterstützt: **WPA Pre-Shared Key** (WPA Vorläufiger gemeinsamer Schlüssel), **WPA RADIUS**, **RADIUS** und **WEP**. (WPA steht für *Wi-Fi Protected Access*; dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung. WEP steht für *Wired Equivalent Privacy* und RADIUS für *Remote Authentication Dial-In User Service*.) Im Folgenden erhalten Sie einen Überblick über diese vier Sicherheitsstandards. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Routers erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.

WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel): Bei WPA steht Ihnen die Verschlüsselungsmethode TKIP mit dynamischen Verschlüsselungsschlüsseln zur Verfügung. Wählen Sie den Algorithmus **TKIP** aus: Geben Sie einen gemeinsamen WPA-Schlüssel mit einer Länge von 8 bis 32 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Router mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind (siehe Abbildung 5-14).

Abbildung 5-14: WPA Pre-Shared Key (WPA Vorläufiger gemeinsamer Schlüssel)

WPA/RADIUS: Bei dieser Option wird WPA in Kombination mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit dem Router verbunden ist.) Wählen Sie zuerst den gewünschten WPA-Algorithmus aus (**TKIP**). Geben Sie die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch den Router und den Server freigegeben ist. Legen Sie zuletzt den Wert **Key Renewal Timeout** (Wartezeit für Schlüsselerneuerung) fest. Diese Zeitangabe teilt dem Router mit, wie oft die Verschlüsselungsschlüssel auszutauschen sind (siehe Abbildung 5-15).

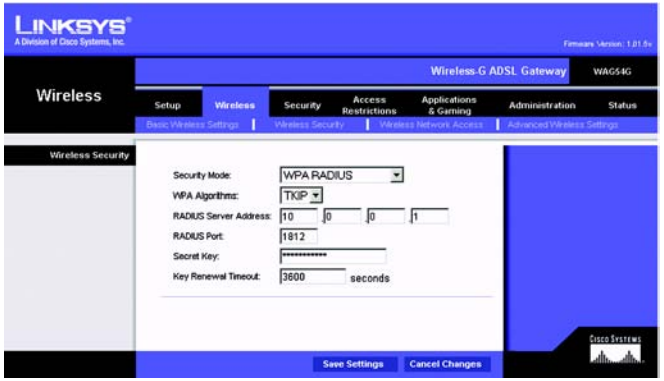

Abbildung 5-15: WPA RADIUS

RADIUS: Bei dieser Option wird WEP in Kombination mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit dem Router verbunden ist.) Geben Sie zuerst die IP-Adresse des RADIUS-Servers in das Feld **RADIUS Server Address** (Adresse des RADIUS-Servers) und die Portnummer in das Feld **RADIUS Port** (RADIUS-Port) sowie den Schlüssel in das Feld **Shared Key** (Freigegebener Schlüssel) ein, der für die Verwendung durch den Router und den Server freigegeben ist. Wählen Sie anschließend als WEP-Verschlüsselungsebene **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) und den Wert für **Default Key** (Standard-Schlüssel) (wählen Sie den gewünschten Schlüssel aus) aus. Erstellen Sie zuletzt einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben (siehe Abbildung 5-16).

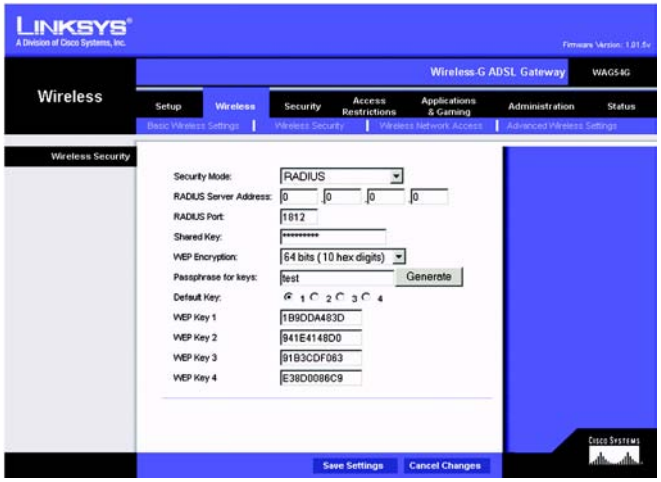

Abbildung 5-16: RADIUS

WEP: WEP ist eine grundlegende Verschlüsselungsmethode, die nicht so sicher wie WPA ist. Um WEP zu verwenden, wählen Sie einen Wert für **Default Key** (Standard-Schlüssel) (wählen Sie den gewünschten Schlüssel aus) sowie als WEP-Verschlüsselungsebene **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) aus. Erstellen Sie anschließend einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben (siehe Abbildung 5-17).

- Ändern Sie die Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen anzuwenden, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Routers erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.
- **WEP Encryption Level** (WEP-Verschlüsselungsebene): WEP ist die Abkürzung für *Wired Equivalent Privacy.* Hierbei handelt es sich um eine Verschlüsselungsmethode zum Schutz der Wireless-Datenkommunikation. WEP basiert auf einem 64-Bit oder 128-Bit-Schlüssel zur Steuerung des Zugriffs auf Ihr Netzwerk und zur höheren Sicherheit durch Verschlüsselung der Datenübertragung. Um übertragene Daten zu entschlüsseln, müssen alle Geräte im Netzwerk den gleichen WEP-Schlüssel verwenden. Höhere Verschlüsselungsebenen bieten eine höhere Sicherheitsstufe, durch die Komplexität der Verschlüsselung kann jedoch die Netzwerkleistung vermindert werden. Um WEP zu aktivieren, wählen Sie **64 bits (10 hex digits)** (64 Bits 10 Hexadezimalziffern) (siehe Abbildung 5-13) oder **128 bits (26 hex digits)** (128 Bits 26 Hexadezimalziffern) (siehe Abbildung 5-14) aus.
- **Passphrase for keys** (Schlüssel-Passphrase): Sie können anstelle der manuellen Eingabe von WEP-Schlüssels eine Passphrase eingeben. Mit dieser Passphrase können Sie mindestens einen WEP-Schlüssel erstellen. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Diese Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Um mit Wireless-Produkten anderer Hersteller oder mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung zu kommunizieren, notieren Sie sich den im Feld **WEP Key 1** (Schlüssel 1) generierten WEP-Schlüssel und geben ihn manuell in den Wireless-Client ein.) Klicken Sie nach Eingabe der Passphrase auf **Generate** (Generieren), um WEP-Schlüssel zu erstellen.
- **Default Key** (Standard-Schlüssel): Legen Sie fest, welcher WEP-Schlüssel (1 bis 4) verwendet werden soll, wenn Daten über das Gateway übertragen werden. Stellen Sie sicher, dass das Empfangsgerät (Wireless-Client) den gleichen Schlüssel verwendet.
- **WEP Keys 1-4** (WEP-Schlüssel 1 - 4): Mithilfe von WEP-Schlüsseln können Sie ein Verschlüsselungsschema für Übertragungen im Wireless-Netzwerk erstellen. Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie ein Schlüsselfeld nicht leer, und geben Sie nicht in alle Schlüsselfelder den Wert 0 ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie eine 64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 hexadezimale Zeichen betragen. Wenn Sie eine 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zeichen von 0 bis 9 und von A bis F.

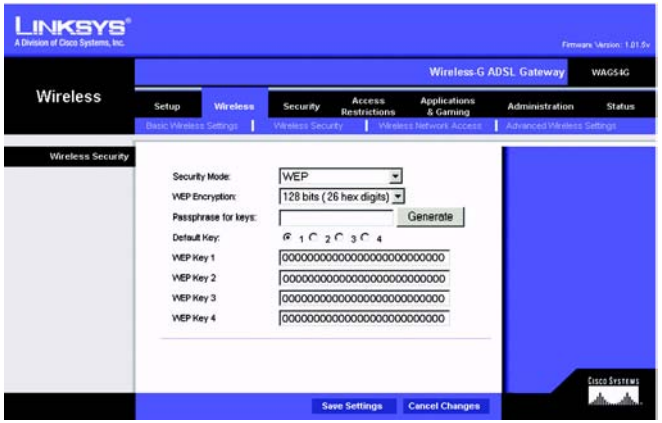

Abbildung 5-17: WEP

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Wireless Netzwork Access (Wireless-Netzwerkzugriff) (siehe Abbildung 5-18)

Wireless Network Access (Wireless-Netzwerkzugriff): Wenn Sie die Option **Allow All** (Alle zulassen) auswählen, haben alle Computer Zugriff auf das Wireless-Netzwerk. Wählen Sie die Option **Restrict Access** (Zugriff beschränken) aus, um den Zugriff auf das Netzwerk zu beschränken. Klicken Sie auf die Schaltfläche **Select MAC Address From Networked Computers** (MAC-Adresse von Netzwerk-PCs auswählen), um das in Abbildung 5-19 aufgeführte Fenster anzuzeigen.

Wählen Sie aus der Liste den Eintrag **MAC Address** (MAC-Adresse) aus, aktivieren Sie das Kontrollkästchen **Select** (Auswahl), und klicken Sie auf die Schaltfläche **Select** (Auswahl).

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

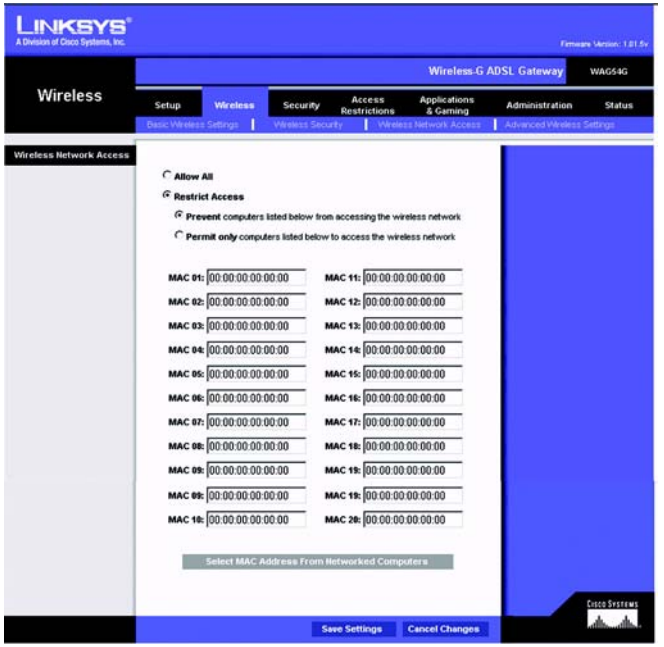

Abbildung 5-18: Wireless Network Access (Wireless-Netzwerkzugriff)

Abbildung 5-19: Networked Computers (Netzwerk-Computer)

Die Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)
(siehe Abbildung 5-20)

Sie können über dieses Fenster auf die folgenden erweiterten Wireless-Funktionen zugreifen: **Authentication Type** (Authentifizierungstyp), **Basic Data Rates** (Basis-Datenrate), **Control Tx Rates** (Gesteuerte Übertragungsraten), **Beacon Interval** (Beacon-Intervall), **DTIM Interval** (DTIM-Intervall), **RTS Threshold** (RTS-Schwelle) und **Fragmentation Threshold** (Fragmentierungsschwelle).

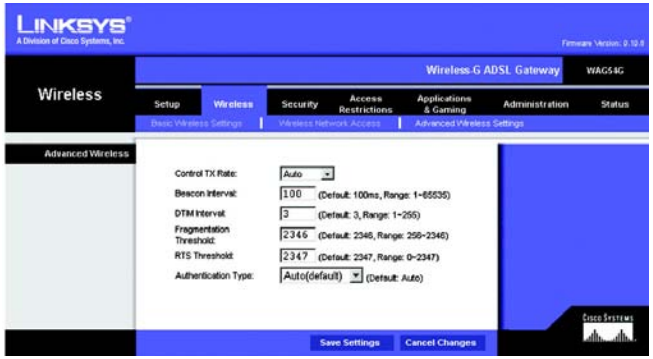

Abbildung 5-20: Advanced Wireless Settings (Erweiterte Wireless-Einstellungen)

- **Control Tx Rates** (Gesteuerte Übertragungsraten): Die Standardübertragungsrate ist auf **Auto** (Automatisch) festgelegt. Der Bereich liegt zwischen 1 und 54 MBit/s. Die Datenübertragungsrate sollte gemäß der Geschwindigkeit des Wireless-Netzwerks eingestellt werden. Sie können aus einer Reihe von Übertragungsgeschwindigkeiten auswählen oder die standardmäßig eingestellte Option **Auto** (Automatisch) beibehalten, mit der das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt.
- **Beacon Interval** (Beacon-Intervall): Der Standardwert ist 100. Geben Sie einen Wert zwischen 1 und 65.535 Millisekunden ein. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paketübertragung des Gateways zur Synchronisierung des Wireless-Netzwerks.
- **DTIM Interval** (DTIM-Intervall): Der Standardwert ist 3. Der Wert (zwischen 1 und 255) gibt das Intervall der DTIM (*Delivery Traffic Indication Message*) an. Ein DTIM-Feld ist ein Zeitkontrollfeld, das die Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet er die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit.
- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert sollte bei dem Standardwert von 2346 belassen werden. Der Bereich liegt bei 256 bis 2346 Byte. Er gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Wenn die Fragmentierungsschwelle zu niedrig liegt, kann dies zu einer Verringerung der Netzwerkleistung führen. Es wird nur eine geringfügige Senkung dieses Werts empfohlen.
- **RTS Threshold** (RTS-Schwelle): Dieser Wert sollte bei dem Standardwert von 2347 belassen werden. Der Bereich liegt bei 0 bis 2347 Byte. Bei einem schwankenden Datenfluss wird eine nur geringfügige Senkung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*RTS = Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Daten-Blocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*CTS = Clear to Send*), um das Recht, mit der Übertragung zu beginnen, anzuerkennen.
- **Authentication Type** (Authentifizierungstyp): Standardmäßig ist die Option **Auto** (Automatisch, Standard) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Freigegebener Schlüssel) verwendet werden kann. Beim Authentifizierungstyp **Open System** (Offenes System) verwenden Absender und Empfänger zur Authentifizierung keinen WEP-Schlüssel, sondern WEP zur Datenverschlüsslung. Wenn Sie nur den Open System-Authentifizierungstyps verwenden möchten, wählen Sie die Option **Open System** (Offenes System) aus. Beim Authentifizierungstyp **Shared Key** (Freigegebener Schlüssel) verwenden Absender und Empfänger sowohl zur Authentifizierung als auch zur Datenverschlüsselung einen WEP-Schlüssel. Wenn Sie nur den Shared Key-Authentifizierungstyp verwenden möchten, wählen Sie die Option **Shared Key** (Freigegebener Schlüssel) aus. Es wird empfohlen, diese Option auf dem Standardmodus **Auto** (Automatisch) zu belassen, da einige Clients nicht für die Option **Shared Key** (Freigegebener Schlüssel) konfiguriert werden können.

Die Registerkarte „Security“ (Sicherheit)

Firewall

Wenn Sie auf die Registerkarte „Security“ (Sicherheit) klicken, wird das Fenster **Firewall** angezeigt (siehe Abbildung 5-21). Dieses Fenster enthält Filter und die Option zum Blockieren von WAN-Anfragen. Durch die Verwendung von Filtern können spezielle Internetdatentypen und anonyme Internet-Anfragen geblockt werden.

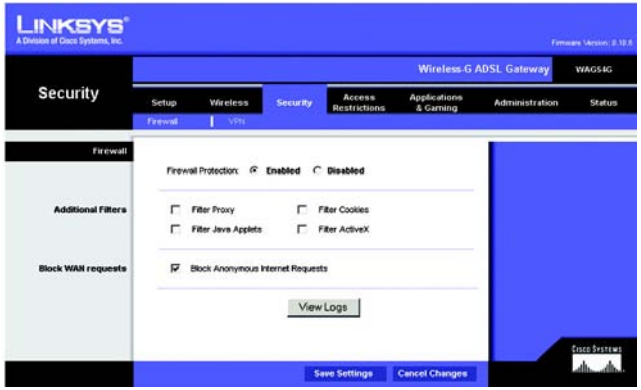

Abbildung 5-21: Firewall

- **Firewall** (Firewall): Klicken Sie zum Hinzufügen des Firewall-Schutzes auf **Enabled** (Aktiviert). Klicken Sie zum deaktivieren des Firewall-Schutzes auf **Disabled** (Deaktiviert).

  Additional Filters (Zusätzliche Filter)

- **Filter Proxy** (Filterproxy): Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie den Filterproxy ablehnen, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Um die Proxy-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Internetsites beim Zugriff auf diese Sites verwendet werden. Um die Cookie-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, haben Sie möglicherweise keinen Zugriff auf Internetsites, die mit dieser Programmiersprache erstellt wurden. Um die Java Applet-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, haben Sie möglicherweise keinen Zugriff auf Internetsites, die mit dieser Programmiersprache erstellt wurden. Um die ActiveX-Filterung zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).

  Block WAN Requests (WAN-Anfragen blockieren)

- **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren): Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit Ihres Netzwerks erhöhen, indem Ihre Netzwerk-Ports nicht angezeigt werden und Ihr Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen), um Protokolle von Firewall-Ereignissen anzuzeigen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

VPN (*Virtual Private Networking*)

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, durch die eine sichere Verbindung zwischen zwei entfernten Standorten erstellt wird. Über das in Abbildung 5-22 aufgeführte Fenster können Sie Ihre VPN-Einstellungen konfigurieren, um dadurch die Sicherheit Ihres Netzwerks zu erhöhen.

VPN Passthrough (VPN-Passthrough)

- **IPSec Passthrough** (IPSec-Passthrough): IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zur Implementierung eines sicheren Paketaustauschs auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enabled** (Aktiviert). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).
- **PPTP Passthrough** (PPTP-Passthrough): PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf einem Windows NT 4.0- oder Windows 2000-Server. Um PPTP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enabled** (Aktiviert). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).

IPSec VPN Tunnel (IPSec VPN-Tunnel)

Das VPN-Gateway erstellt einen Tunnel bzw. Kanal zwischen zwei Endpunkten, so dass die Datenübertragungen zwischen diesen beiden Endpunkten sicher sind.

- Um den Tunnel festzulegen, wählen Sie den Tunnel, den Sie erstellen möchten, aus der Dropdown-Liste **Select Tunnel Entry** (Tunneleintrag auswählen) aus. Es können bis zu 5 gleichzeitig aktive Tunnel erstellt werden. Klicken Sie anschließend auf **Enabled** (Aktiviert), um den IPSec VPN-Tunnel zu aktivieren. Wenn der Tunnel aktiviert ist, geben Sie den Namen des Tunnels in das Feld **Tunnel Name** (Tunnelname) ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird.
- **Local Secure Group** (Lokale sichere Gruppe) und **Remote Secure Group** (Entfernte sichere Gruppe): Die **Local Secure Group** (Lokale sichere Gruppe) umfasst die Computer in Ihrem LAN, die auf den Tunnel zugreifen können. Die **Remote Secure Group** (Entfernte sichere Gruppe) umfasst die Computer am entfernten Ende des Tunnels, die auf den Tunnel zugreifen können. Diese Computer können durch ein Subnetz, eine spezielle IP-Adresse oder einen Bereich festgelegt werden.
- **Remote Security Gateway** (Entferntes Sicherheits-Gateway): Bei dem **Remote Security Gateway** (Entferntes Sicherheits-Gateway) handelt es sich um das VPN-Gerät (beispielsweise ein zweites VPN-Gateway) am entfernten Ende des VPN-Tunnels. Geben Sie die IP-Adresse oder Domäne des VPN-Geräts am anderen Ende des Tunnels ein. Bei dem entfernten VPN-Gerät kann es sich um ein anderes VPN-Gateway, einen VPN-Server oder einen Computer mit VPN-Client-Software handeln, der IPSec unterstützt. Bei der IP-Adresse kann es sich je nach den Einstellungen des entfernten VPN-Geräts um eine statische (permanente) Adresse oder um eine dynamische (sich ändernde) Adresse handeln. Vergewissern Sie sich, dass Sie die korrekte IP-Adresse eingegeben haben; anderenfalls kann keine Verbindung hergestellt werden. Denken Sie daran, dass dies NICHT die IP-Adresse des lokalen VPN-Gateways ist, sondern die IP-Adresse des entfernten VPN-Gateways bzw. -Geräts, mit dem kommuniziert werden soll. Wenn Sie eine IP-Adresse eingeben, kann nur mit der angegebenen IP-Adresse auf den Tunnel zugegriffen werden. Wenn Sie **Any** (Alle) auswählen, kann mit jeder IP-Adresse auf den Tunnel zugegriffen werden.

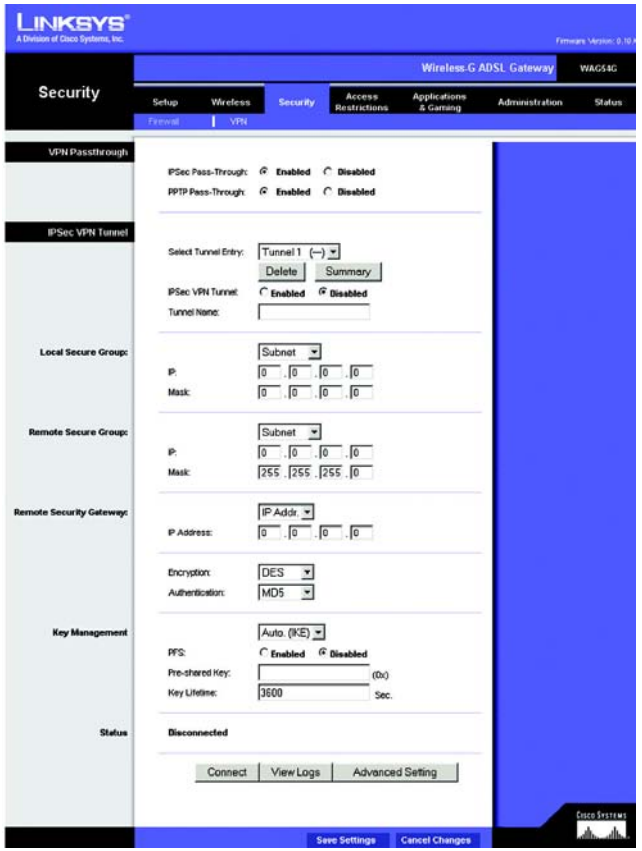

Abbildung 5-22: VPN

- **Encryption** (Verschlüsselung): Mit **Encryption** (Verschlüsselung) machen Sie die Verbindung noch sicherer. Es stehen zwei Verschlüsselungstypen zur Verfügung: DES und 3DES (empfohlen wird 3DES, weil dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Disable** (Deaktivieren) auswählen. In Abbildung 5-22 wurde DES ausgewählt (Standardeinstellung).
- **Authentication** (Authentifizierung): Die Authentifizierung wirkt wie eine weitere Sicherheitsstufe. Es stehen zwei Authentifizierungstypen zur Verfügung: MD5 und SHA (empfohlen wird **SHA**, weil dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit Disable (Deaktivieren) an beiden Enden des Tunnels deaktiviert werden. In Abbildung 5-22 wurde MD5 gewählt (Standardeinstellung).
- **Key Management** (Schlüsselverwaltung): Wählen Sie aus dem Dropdown-Menü **Auto (IKE)** oder **Manual** (Manuell) aus. Beide Methoden werden im Folgenden beschrieben.

  Auto (IKE):
  Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Pre-shared Key** (Vorläufiger gemeinsamer Schlüssel) ein. Wenn dieses Verfahren verwendet wird, MUSS das Wort an beiden Enden des Tunnels eingegeben werden. Auf der Grundlage dieses Worts wird ein Schlüssel erstellt, mit dem die über den Tunnel versendeten Daten verschlüsselt und entschlüsselt werden. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden. Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, so dass der Schlüssel unbegrenzt lange zur Verfügung steht. Markieren Sie das Kontrollkästchen neben **PFS** (Perfect Forward Secrecy) [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind.

  Manual (Manuell): (siehe Abbildung 5-23)
  Wählen Sie **Manual** (Manuell) aus, und wählen Sie anschließend den Verschlüsselungsalgorithmus aus der Dropdown-Liste aus. Geben Sie den Verschlüsselungsschlüssel in das dafür vorgesehene Feld ein (wenn Sie DES als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 16 hexadezimale Zeichen ein, wenn Sie 3DES ausgewählt haben, geben Sie 48 hexadezimale Zeichen ein). Wählen Sie den Authentifizierungsalgorithmus aus der Dropdown-Liste aus. Geben Sie den Authentifizierungsschlüssel in das dafür vorgesehene Feld ein (wenn Sie MD5 als Verschlüsselungsalgorithmus ausgewählt haben, geben Sie 32 hexadezimale Zeichen ein, wenn Sie SHA1 ausgewählt haben, geben Sie 40 hexadezimale Zeichen ein). Geben Sie in die entsprechenden Felder **Inbound SPI** (Eingangs-SPI) und **Outbound SPI** (Ausgangs-SPI) ein.
- **Status**: In dieser Zeile wird der Status der Verbindung angezeigt.

Klicken Sie auf die Schaltfläche **Connect** (Verbinden), um Ihren VPN-Tunnel zu verbinden. Klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen), um Protokolle anzuzeigen. Klicken Sie auf die Schaltfläche **Advanced Setting** (Weitere Einstellungen), um das Fenster **Advanced IPSec VPN Tunnel Setup** (Erweiterte IPSec VPN-Tunnel-Einrichtung) anzuzeigen (siehe Abbildung 5-24).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

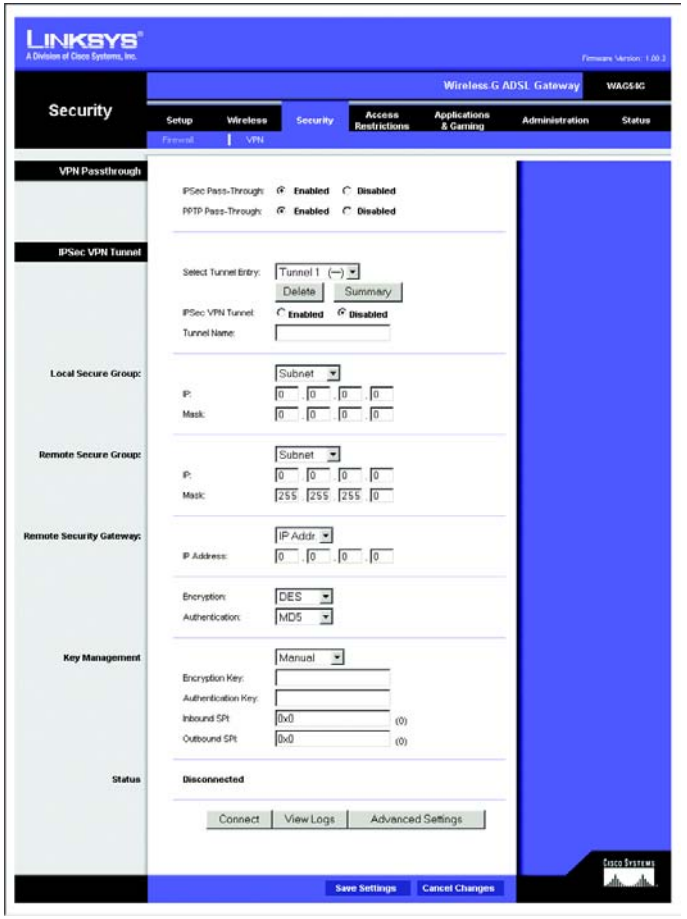

Abbildung 5-23: Manual Key Management (Manuelle Schlüsselverwaltung)

Advanced VPN Tunnel Setup (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Sie können über das in Abbildung 5-24 dargestellte Fenster **Advanced IPSec VPN Tunnel Setup** (Erweiterte IPSec VPN-Tunnel-Einrichtung) die Einstellungen für bestimmte VPN-Tunnel anpassen.

Phase 1

- **Phase 1** wird zur Erstellung einer Sicherheitsverknüpfung, auch „IKE SA“ (*Internet Key Exchange, Security Assosication*) genannt, verwendet. Nach Abschluss von Phase 1 wird in Phase 2 mindestens eine „IPSec SA“ erstellt und für IPSec-Sitzungen verwendet.
- **Operation Mode** (Betriebsmodus): Die beiden verfügbaren Betriebsmodi **Main** (Hauptmodus) und **Aggressive** (Aggressiver Modus) tauschen die gleichen IKE-Nutzlasten auf unterschiedlichen Sequenzen aus. Der Hauptmodus wird häufiger verwendet, wobei einige Anwender jedoch den schnelleren aggressiven Modus vorziehen. Der Hauptmodus kann zur durchschnittlichen Verwendung eingesetzt werden und enthält mehr Authentifizierungserfordernisse als der aggressive Modus. Die Verwendung des Hauptmodus wird empfohlen, da dieser Modus sicherer ist. Bei beiden Modi werden vom VPN-Gateway Anfragen sowohl im Haupt- als auch im aggressiven Modus vom standortfernen VPN-Gerät akzeptiert. Wählen Sie **Username** (Benutzername), und geben Sie den Benutzername ein.
- **Encryption** (Verschlüsselung): Wählen Sie die Länge des Schlüssels aus, der zum Verschlüsseln/Entschlüsseln von ESP-Paketen verwendet wird. Sie können zwischen zwei Verschlüsselungsarten wählen: DES und 3DES.Die Verwendung von 3DES wird empfohlen, da diese Verschlüsselungsart sicherer ist.
- **Authentication** (Authentifizierung): Wählen Sie die Methode aus, die zur Authentifizierung von ESP-Paketen verwendet wird. Sie können zwischen zwei Methoden wählen: MD5 und SHA. Die Verwendung von SHA wird empfohlen, da diese sicherer ist.
- **Group** (Gruppe): Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.
- **Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie optional einen Zeitraum festlegen, wie lange der Schlüssel verfügbar ist, bevor ein abläuft. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, so dass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

Phase 2

- **Encryption** (Verschlüsselung): Die in Phase 1 ausgewählte Verschlüsselungsmethode wird angezeigt.
- **Authentication** (Authentifizierung): Die in Phase 2 ausgewählte Authentifizierungsmethode wird angezeigt.
- **PFS** (PFS, *Perfect Forward Secrecy*): In dieser Zeile wird der PFS-Status angezeigt.
- **Group** (Gruppe): Es stehen zwei Diffie-Hellman-Gruppen zur Auswahl: 768 Bit und 1024 Bit. Der Begriff Diffie-Hellman bezeichnet eine kryptografische Verschlüsselungstechnik, bei der sowohl öffentliche als auch private Schlüssel zur Ver- und Entschlüsselung verwendet werden.
- **Key Life Time** (Schlüssel-Verwendungsdauer): Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, so dass der Schlüssel bis zur erneuten Schlüsselverhandlung zwischen den Endpunkten zur Verfügung steht.

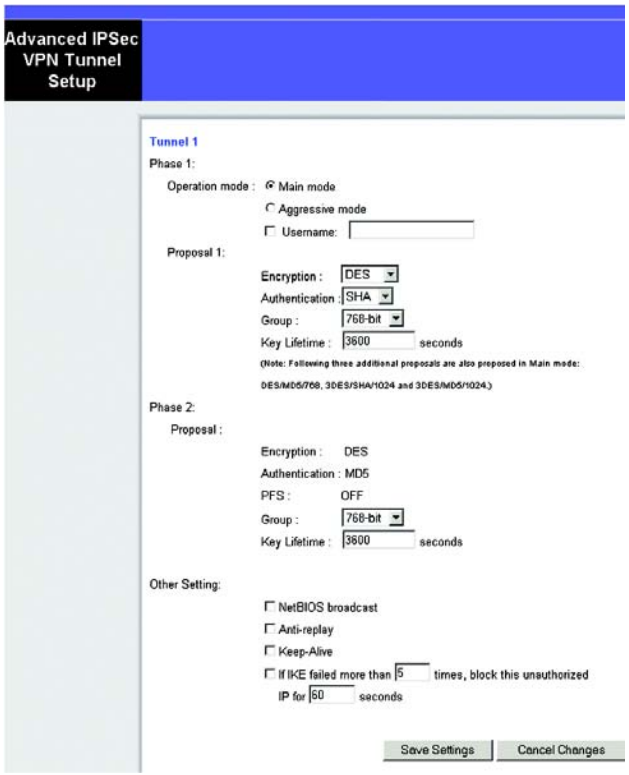

Abbildung 5-24: Advanced VPN Tunnel Setup (Erweiterte IPSec VPN-Tunnel-Einrichtung)

Other Setting (Zusätzliche Einstellung)

- **NetBIOS broadcast** (NetBIOS-Broadcast): Aktivieren Sie das Kontrollkästchen neben **NetBIOS broadcast** (NetBIOS-Broadcast), um den NetBIOS-Datenverkehr durch den VPN-Tunnel zu leiten.
- **Anti-replay** (Anti-Replay): Aktivieren Sie das Kontrollkästchen neben **Anti-replay** (Anti-Replay), um den Anti-Replay-Schutz zu aktivieren. Mithilfe dieser Funktion werden die Sequenznummern der eingehenden Datenpakete aufgezeichnet, wodurch die Sicherheit auf IP-Paketebene gewährleistet wird.
- **Keep-Alive** (Verbindung aufrechterhalten): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her.
- Aktivieren Sie dieses Kontrollkästchen, um unberechtigte IP-Adressen zu blockieren. Füllen Sie dieses Feld aus, um die Anzahl der fehlgeschlagenen IKE festzulegen, bevor die unberechtigte IP-Adresse blockiert wird. Geben Sie den Zeitraum in Sekunden in dieses Feld ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Klicken Sie auf die Schaltfläche **Help** (Hilfe), um weitere Informationen zu dieser Registerkarte zu erhalten.

Die Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

Internet Access (Internetzugriff)

Über die Registerkarte „Access Restrictions“ (siehe Abbildung 5-25) können Sie bestimmte Arten der Internetverwendung blockieren bzw. zulassen. Sie können für bestimmte Computer Sicherheitsrichtlinien für den Internetzugriff und Filter mithilfe von Netzwerk-Anschlussnummern einrichten.

- **Internet Access Policy** (Richtlinien für Internetzugriff): Mehrfache Filter können als Sicherheitsrichtlinien für den Internetzugriff gespeichert werden. Wählen zur Bearbeitung einer Richtlinie die entsprechende Nummer aus der Dropdown-Liste aus. Die Anzeige der Registerkarte ändert sich, um die Änderungen an den Einstellungen an dieser Richtlinie anzuzeigen. Klicken Sie zum Löschen dieser Richtlinie auf die Schaltfläche **Delete** (Löschen). Klicken Sie zur Anzeige einer Zusammenfassung aller Richtiglinien auf die Schaltfläche **Summary** (Zusammenfassung).

  Die Zusammenfassung wird in einem Fenster (siehe Abbildung 5-26) mit dem entsprechenden Namen und den entsprechenden Einstellungen angezeigt. Um zur Registerkarte **Filters** (Filter) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).

- **Enter Policy Name** (Richtliniennamen eingeben): Richtlinien werden auf Grundlage der hier aufgeführten Felder erstellt.

  So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Geben Sie im Feld **Policy Name** (Richtlinienname) einen Namen für die Richtlinie ein. Wählen Sie **Internet Access** (Internetzugriff) als Richtlinientyp aus.

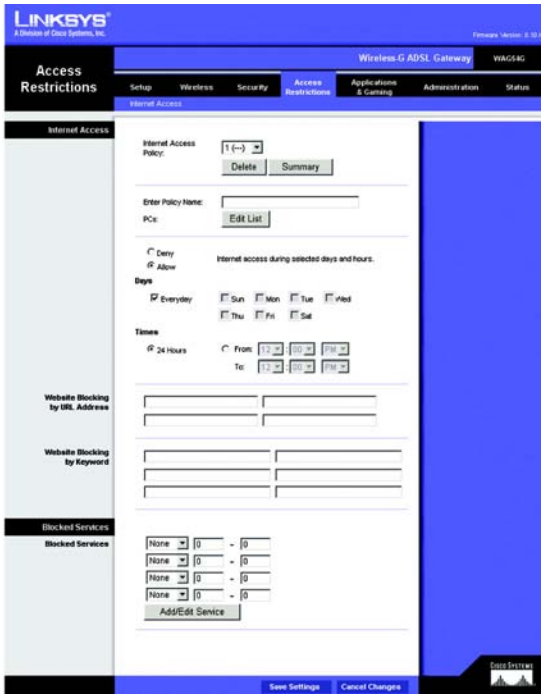

Abbildung 5-25: Access Restriction (Zugriffsbeschränkungen)

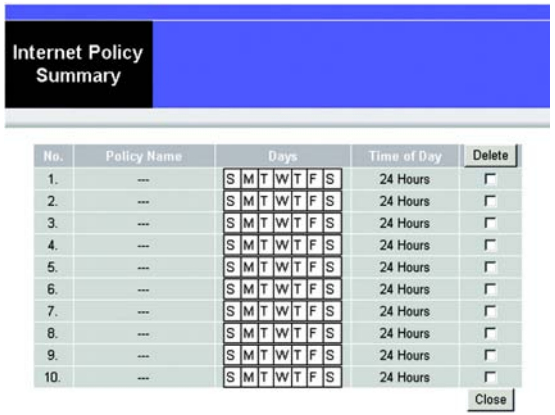
Internet Policy Summary
No.
Policy Name
Days
Time of Day
Delete
1. --- S M T W T F S 24 Hours
2. --- S M T W T F S 24 Hours
3. --- S M T W T F S 24 Hours
4. --- S M T W T F S 24 Hours
5. --- S M T W T F S 24 Hours
6. --- S M T W T F S 24 Hours
7. --- S M T W T F S 24 Hours
8. --- S M T W T F S 24 Hours
9. --- S M T W T F S 24 Hours
10. --- S M T W T F S 24 Hours
Close

Abbildung 5-26: Internet Policy Summary (Internet-Richtlinien - Zusammenfassung)

2. Klicken Sie auf die Schaltfläche **Edit List** (Liste bearbeiten). Dadurch wird ein Fenster angezeigt, in dem die PC-Liste aufgeführt ist (siehe Abbildung 5-27). In diesem Feld können Sie die IP-Adresse bzw. MAC-Adresse der Computer angeben, auf die die Richtlinie angewendet werden soll. Sie können auch über die IP-Adresse Computerbereiche eingeben. Klicken Sie auf die Schaltfläche **Apply** (Anwenden), um Ihre Einstellungen zu speichern, auf die Schaltfläche **Cancel** (Abbrechen), um Änderungen rückgängig zu machen, und die Schaltfläche **Close** (Schließen), um zur Registerkarte **Filters** (Filter) zurückzukehren.

3. Klicken Sie auf die entsprechende Option [**Deny** (Verweigern) oder **Allow** (Zulassen)], um den Internetzugriff für die PCs, die im Fenster **List of PCs** (PC-Liste) aufgeführt sind, zu blockieren oder zuzulassen.

4. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet zugegriffen werden kann, wie z. B. FTP oder Telnet, indem Sie diese Dienste in den Dropdown-Menüs neben **Blocked Services** (Blockierte Dienste) auswählen. Wenn ein Dienst nicht in der Liste aufgeführt ist, klicken Sie auf die Schaltfläche **Add/Edit Service** (Dienst hinzufügen/bearbeiten), um das Fenster **Port Services** (Anschlussdienste) (siehe Abbildung 5-28) zu öffnen und der Liste einen Dienst hinzuzufügen. Sie müssen einen Dienstnamen und das von diesem Dienst verwendete Protokoll sowie den Anschlussbereich eingeben.

5. Durch Auswahl der entsprechenden Zeit- und Datumseinstellung legen Sie den Zeitpunkt fest, zu dem der Internetzugriff gefiltert wird.

6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Richtlinie zu aktivieren.

Der Internetzugriff kann auch über die URL-Adresse gefiltert werden, die Sie für den Zugriff auf Internetadressen eingegeben haben. Geben Sie hierfür die Adresse in eines der Felder **Website Blocking by URL Address** (Website nach URL-Adresse blockieren) ein. Wenn Ihnen die URL-Adresse nicht bekannt ist, können Sie das Filtern mithilfe bestimmter Stichwörter vornehmen. Geben Sie hierfür ein Stichwort in eines der Felder **Website Blocking by Keyword** (Website nach Schlüsselwort blockieren) ein.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

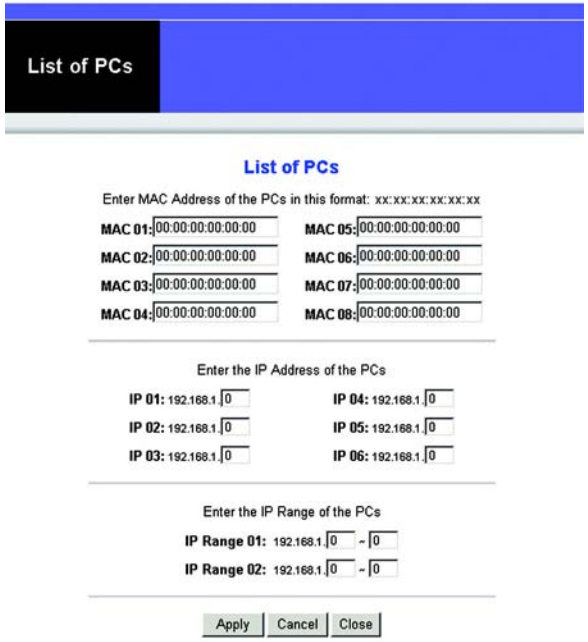

Abbildung 5-27: List of PCs (PC-Liste)

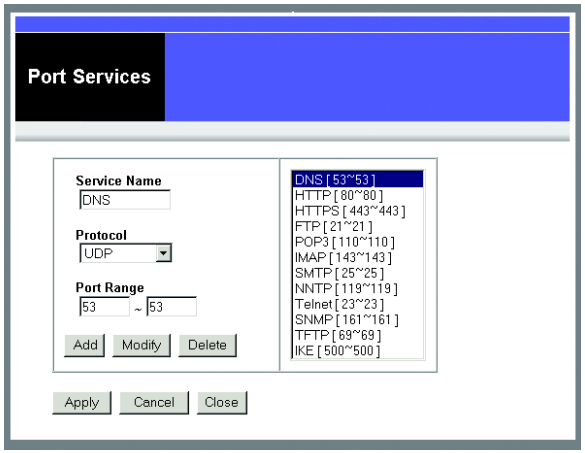

Abbildung 5-28: Port Services (Anschlussdienste)

Die Registerkarte „Applications and Gaming“ (Anwendungen und Spiele)

Single Port Forwarding (Einfaches Port-Forwarding)

Das Fenster **Single Port Forwarding** (Einfaches Port-Forwarding) bietet Optionen zur Anpassung der Anschlussdienste der gängigsten Anwendungen (siehe Abbildung 5-29).

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

Wählen Sie in diesem Feld eine Anwendung aus, oder geben Sie eine Anwendung ein. Geben Sie in diese Felder anschließend die Anschlussnummern der externen und internen Anschlüsse an. Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP** oder **UDP**. Geben Sie in das Feld die IP-Adresse ein. Klicken Sie auf **Enabled** (Aktiviert), um das UPnP-Forwarding für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

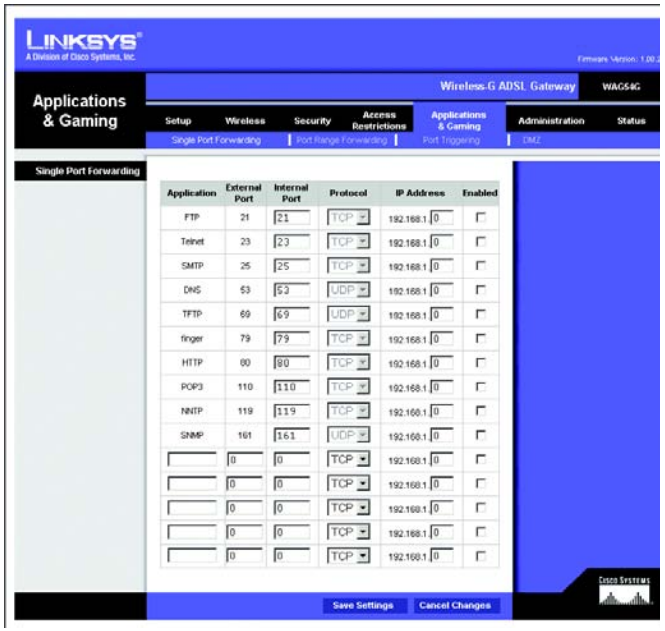

Abbildung 5-29: Single Port Forwarding (Einfaches Port-Forwarding)

Port Range Forwarding (Weiterleitung an einen Anschlussbereich)

Im Fenster **Port Forwarding** (Port-Forwarding) können Sie öffentliche Dienste auf Ihrem Netzwerk, wie z. B. Web-, FTP-, E-Mail-Server oder spezielle Internet-Anwendungen, festlegen. (Unter speziellen Internet-Anwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internet-Anwendungen ist keine Weiterleitung erforderlich (siehe Abbildung 5-30).

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein; darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start** (Von) und **End** (Bis): Geben Sie die Anfangs- und Endnummern der Ports ein, die weitergeleitet werden sollen
- **TCP** und **UDP**: Wählen Sie den Protokolltyp aus, den Sie für jede Anwendung verwenden möchten: **TCP**, **UDP** oder **Both** (Beide).
- **IP Address** (IP-Adresse): Geben Sie die IP-Adresse ein, und klicken Sie auf **Enabled** (Aktiviert).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

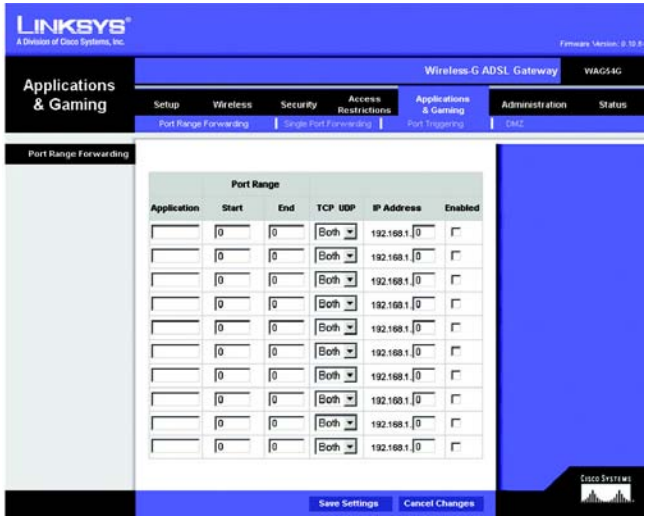

Abbildung 5-30: Port Range Forwarding (Weiterleitung an einen Anschlussbereich)

Port Triggering (Port-Triggering)

Port-Triggering wird bei speziellen Anwendungen verwendet, über die ein Anschluss auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Anschlussnummern (siehe Abbildung 5-31). Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln dem richtigen Computer weitergeleitet.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Start Port** (Start-Port) und **End Port** (End-Port): Geben Sie Anfang und Ende der Bereichsnummern für Ausgangs-Port-Triggering sowie die Bereichsnummern für Port-Forwarding der Anschlüsse ein, die Sie weiterleiten möchten.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

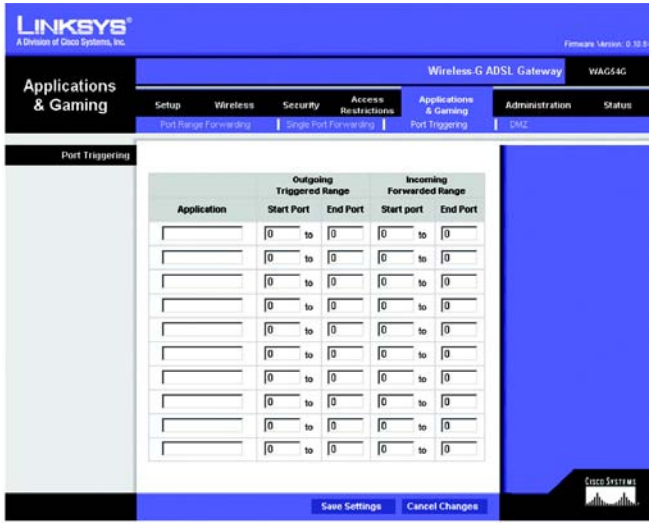

Abbildung 5-31: Port-Triggering

DMZ

Über das Fenster **DMZ** (siehe Abbildung 5-32) kann mithilfe von DMZ-Hosting für einen Netzwerkbenutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Mit DMZ-Hosting werden alle Anschlüsse gleichzeitig an einen PC weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

- „DMZ Hosting“ (DMZ-Hosting): Mit der DMZ-Funktion (*DMZ = Demilitarized Zone*; entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Enabled** (Aktiviert), um diese Funktion zu verwenden. Klicken Sie auf **Disabled** (Deaktiviert), um die DMZ-Funktion zu deaktivieren.
- „DMZ Host IP Address“ (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln einer IP-Adresse finden Sie in „Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

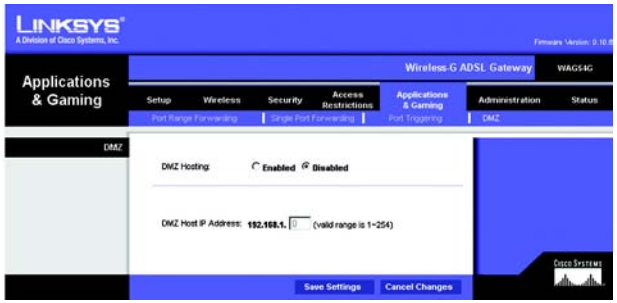

Abbildung 5-32: DMZ

Die Registerkarte „Administration“ (Verwaltung)

Management (Verwaltungsfunktionen)

Über das Fenster **Management** (Verwaltungsfunktionen) (siehe Abbildung 5-33) können Sie die Einstellungen für den Gatewayzugriff sowie die SNMP (Simple Network Management Protocol)- und UPnP (Universal Plug and Play)-Einstellungen ändern.

Abbildung 5-33: Management (Verwaltungsfunktionen)

Gateway Access (Gateway-Zugriff)

Local Gateway Access (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Kennworts aufgefordert. Der Standardbenutzername und das Standardkennwort sind **admin**.

- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen ein: **admin**. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Kennwort): Es wird empfohlen, dass Sie Ihr Standardkennwort in ein persönliches Kennwort ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Kennwort nochmals ein, um es zu bestätigen.

Remote Gatway Access (Entfernter Gateway-Zugriff): Mit dieser Funktion können Sie auf das Gateway von einem entfernten Standort aus über das Internet zugreifen.

WICHTIG: Durch Aktivieren der Funktion **Remote Administration** (Entfernte Verwaltung) ist es jedem Benutzer, der auf Ihr Kennwort zugreifen kann, möglich, das Gateway von jedem beliebigen Standort im Internet aus zu konfigurieren.

- **Remote Administration** (Entfernte Verwaltung): Mit dieser Funktion können Sie das Gateway von einem entfernten Standort aus über das Internet verwalten. Um **Remote Administration** (Entfernte Verwaltung) zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Administration Port** (Verwaltungsanschluss): Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.

SNMP (Simple Network Management Protocol)

SNMP ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung.

Identification (Identifikation): Um SNMP zu verwenden, klicken Sie auf **Enabled** (Aktiviert). Um SNMP zu deaktivieren, klicken Sie auf **Disabled** (Deaktiviert).

- Geben Sie im Feld **Device Name** (Gerätename) den Namen des Gateways ein.
- **Get Community** (Gemeinschaft abrufen): Geben Sie das Kennwort ein, mit dem ein schreibgeschützter Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Gemeinschaft einrichten): Geben Sie das Kennwort ein, mit dem ein Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.

UPnP (Universal Plug and Play)

Mit UPnP kann unter Windows XP das Gateway automatisch für verschiedene Internet-Anwendungen, wie z. B. Internet-Spiele oder Videokonferenzen, konfiguriert werden.

UPnp (Universal Plug and Play): Um UPnP zu verwenden, klicken Sie auf **Enabled** (Aktiviert).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

Reporting (Berichtaufzeichnung)

Über die Registerkarte **Reporting** (Berichtaufzeichnung) (siehe Abbildung 5-34) steht ein Protokoll zur Verfügung, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für Ihre Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN und Firewall-Ereignisse zur Verfügung.

Log (Protokoll)

Log (Protokoll): Um die Berichtaufzeichnung zu verwenden, klicken Sie auf **Enabled** (Aktiviert).

- **Logviewer IP Address** (Logviewer-IP-Adresse): Geben Sie in dieses Feld die IP-Adresse ein, um Protokolle empfangen zu können.

Email Alerts (E-Mail-Warnungen)

Email Alerts (E-Mail-Warnungen): Um E-Mail-Warnungen zu verwenden, klicken Sie auf die Option **Enabled** (Aktiviert).

- **Denial of Service Thresholds** (DoS-Schwellwerte): Geben Sie die Schwellwerte der Ereignisse an, die Sie empfangen möchten.
- **SMTP Mail Server** (SMTP Mail-Server): Geben Sie in dieses Feld die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie in dieses Feld die E-Mail-Adresse für die Warnungsprotokolle ein.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die E-Mail-Adresse für Antwort-E-Mails ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

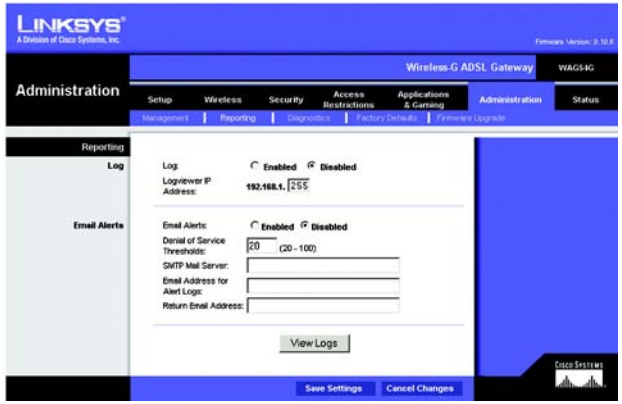

Abbildung 5-34: Reporting (Berichtaufzeichnung)

Diagnostics (Diagnose)

Ping Test (Ping-Test) (siehe Abbildung 5-35)

„Ping Test Parameters“ (Ping-Test-Parameter)

- **Ping Target IP** (Ping-Ziel-IP-Adresse): Geben Sie in dieses Feld die IP-Adresse ein, die Sie für den Ping-Befehl verwenden möchten. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping Size** (Ping-Größe): Geben Sie die Größe des Ping-Pakets an.
- **No. of Pings** (Anzahl der Pings): Geben Sie die Anzahl der Pings an, die durchgeführt werden soll.
- **Ping Interval** (Ping-Intervall): Geben Sie das Ping-Intervall in Millisekunden an.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Wartezeit in Millisekunden an.
- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Klicken Sie auf die Schaltfläche **Start Test** (Test starten), um den Ping-Test zu starten.

Abbildung 5-35: Ping Test (Ping-Test)

Factory Defaults (Werkseinstellungen) (siehe Abbildungen 5-36)

Restore Factory Defaults (Werkseinstellungen wiederherstellen): Wenn Sie alle verfügbaren Optionen angewandt haben und das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Yes** (Ja).

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, kicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) bzw. klicken Sie auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

Abbildung 5-36: Factory Defaults (Werkseinstellungen)

„Firmware Upgrade“ (Firmware aktualisieren) (siehe Abbildung 5-37)

So aktualisieren Sie die Gateway-Firmware:

1. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der Website von Linksys heruntergeladen und extrahiert haben.
2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung 5-37: Firmware Upgrade (Firmware aktualisieren)

Die Registerkarte „Status“ (Status)

Gateway

In diesem Fenster werden Informationen zu Ihrem Gateway und den WAN-Internetverbindungen angezeigt (siehe Abbildung 5-38).

Gateway Information (Gateway-Informationen)

Im Bereich der Gateway-Informationen sind Angaben zur Software-Version, MAC-Adresse und zur derzeitigen Zeit enthalten.

Internet Connections (Internet-Verbindungen)

Im Bereich der Internet-Verbindungen sind Angaben zu ADSL-Link, PPP-Login, Internet-IP-Adresse, öffentliche Subnetzmaske, Standard-Gateway, Primärer DNS-Server sowie zum Ablauf der DHCP-IP-Adresse enthalten.

System Statistics (Systemangaben)

Im Bereich der Systemangaben sind Angaben zu gesendeten und empfangenen Datenpaketen enthalten.

DHCP Renew (DHCP erneuern): Klicken Sie auf die Schaltfläche **DHCP Renew** (DHCP erneuern), um die aktuelle IP-Adresse Ihres Gateways durch eine neue IP-Adresse zu ersetzen.

DHCP Release (DHCP löschen): Klicken Sie auf die Schaltfläche **DHCP Release** (DHCP löschen), um die aktuelle IP-Adresse Ihres Gateways zu löschen.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren.

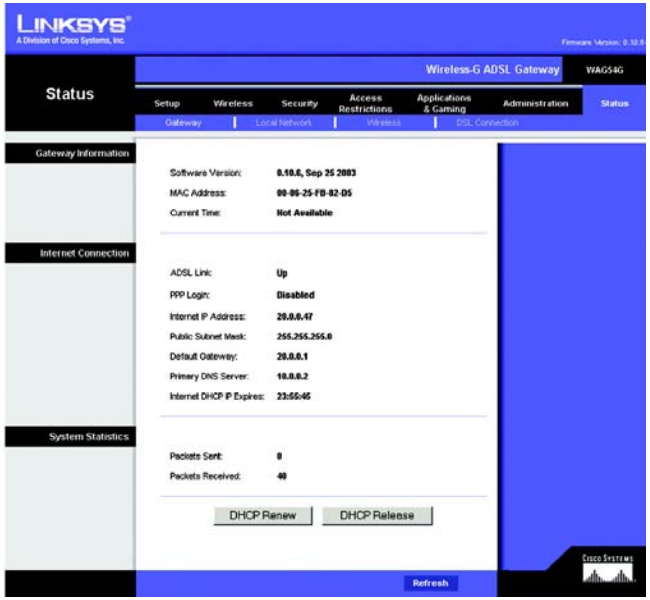

Abbildung 5-38: Status

Local Network (Lokales Netzwerk)

Im Bereich der Angaben zum lokalen Netzwerk sind Informationen zur lokalen Mac-Adresse, IP-Adresse, Subnetzmaske und zum DHCP-Server aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP Client Table** (DHCP-Client-Tabelle) (siehe Abbildung 5-39).

DHCP Client Table (DHCP-Client-Tabelle): Klicken Sie auf die Schaltfläche **DHCP Client Table** (DHCP-Client-Tabelle), um die aktuellen DHCP-Client-Daten aufzurufen. In diesem Bereich sind MAC-Adresse, Computername sowie IP-Adresse der Netzwerk-Clients, die den DHCP-Server verwenden, aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Siehe Abbildung 5-40.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren.

Abbildung 5-39: Local Network (Lokales Netzwerk)

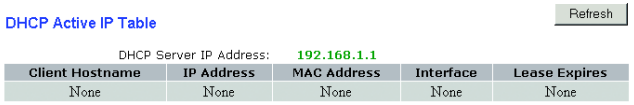

Abbildung 5-40: DHCP-Client-Tabelle

„Wireless“ (Wireless-Netzwerk)

Im Bereich der Wireless-Netzwerkinformationen sind Angaben zu Wireless-Firmware-Version, MAC-Adresse, Status, Modus, Kanal, SSID sowie Verschlüsselung aufgeführt (siehe Abbildung 5-41).

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Wireless-Clients verbunden), um die Wireless-Clients anzuzeigen, die mit dem Gateway verbunden sind.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren.

Abbildung 5-41: Local Network (Wireless-Netzwerk)

DSL Connection (DSL-Verbindung)

Im Bereich der DSL-Verbindung sind Informationen zu Status, Downstream-Rate, Upstream-Rate, Kapselungsmethode, VPI (*Virtual Path Identifier*, Virtueller Pfadidentifizierer), VCI (*Virtual Channel Identifier*, Virtueller Kanalidentifizierer) sowie Multiplexing aufgeführt (siehe Abbildung 5-42).

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Anzeige zu aktualisieren.

Abbildung 5-42: DSL Connection (DSL-Verbindung)

Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: „Behebung häufig auftretender Probleme“ und „Häufig gestellte Fragen“. Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

Behebung häufig auftretender Probleme

1. ***Wie lege ich eine statische IP-Adresse auf einem Computer fest?***
   Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:
   - Für Benutzer von Windows 98 und ME:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
     2. Wählen Sie im Feld **Die folgenden Netzwerkkomponenten sind installiert** die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile „TCP/IP“ ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
     3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften in der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
     4. Klicken Sie auf die Registerkarte **Gateway** und geben Sie 192.168.1.1 ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
     5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass DNS aktiviert ist. Geben Sie den Host- und den Domänennamen ein (z. B. „Johann“ als Hostname und „home“ als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
     6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster **Netzwerk** zu schließen.
     7. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.
   - Für Benutzer von Windows 2000:
     1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk und DFÜ-Verbindungen**.
     2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
     3. Wählen Sie im Feld **Aktivierte Komponenten werden von dieser Verbindung verwendet** die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
     4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
     5. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
     6. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).

7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK** sowie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.
  1. Klicken Sie auf **Start** und **Systemsteuerung**.
  2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
  3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
  4. Wählen Sie im Feld **Diese Verbindung verwendet folgende Elemente** die Option **Internetprotokoll (TCP/IP)**. Klicken Sie auf die Schaltfläche **Eigenschaften**.
  5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
  6. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
  7. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
  8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  9. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK**. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.

2. Ich möchte meine Internetverbindung prüfen.

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in „Kapitel 4: Konfigurieren der Computer“. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option zum automatischen Beziehen einer IP-Adresse von einem DHCP-Server (**IP-Adresse automatisch beziehen**) ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster **Netzwerk** auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie in das Feld **Öffnen** den Eintrag **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie in die Eingabeaufforderung den Eintrag **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie in die Eingabeaufforderung den Eintrag **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie den Eintrag **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie in die Eingabeaufforderung den Eintrag **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Internet verbunden. Wenn Sie KEINE Webseite öffnen können, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.
- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.

- Lesen Sie sich den oben aufgeführten Abschnitt „2. Ich möchte meine Internetverbindung prüfen“ durch, und überprüfen Sie anhand dessen Ihre Verbindung.
    1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: RFC 1483 Bridged (RFC 1483-Überbrückung), RFC 1483 Routed (RFC 1483-Übertragung), RFC 2516 PPPoE oder RFC 2364 PPPoA. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in „Kapitel 5: Konfigurieren des Gateways“ im Abschnitt zur Einrichtung.
    2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob in der Spalte für das Gateway die ADSL-LED konstant leuchtet.
    3. Stellen Sie sicher, dass das an den ADSL-Port Ihres Gateways angeschlossene Kabel in die Wandbuchse der ADSL-Verbindung eingesteckt ist. Überprüfen Sie, dass in der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse Ihres ISP aufgeführt ist.
    4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

4. Ich kann auf die Setup-Seite des webbasierten Dienstprogramms des Gateways nicht zugreifen.

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter „2. Ich möchte meine Internetverbindung prüfen“.
    1. Informationen zur Überprüfung, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in „Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
    2. Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“.
    3. Folgen Sie den Anweisungen unter „10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?“.

5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen; je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.
- Ändern Sie die IP-Adresse des Gateways auf ein anderes Subnetz, so dass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei „X“ für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei „X“ mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways zu 192.168.2.1. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine IP-Adresse dementsprechend zu 192.168.2.Y (wobei „Y“ für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Port 500/UDP-Pakete an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter „7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internet-Anwendungen verwenden.“
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP Ausgang) sowie Port 110 (POP3 Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um Port-Forwarding über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mail-Servern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang D: Ermitteln der MAC-Adresse und IP-Adresse des Ethernet-Adapters“.
  6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
Webserver	80 bis 80	X		192.168.1.100	X
FTP-Server	21 bis 21	X		192.168.1.101	X
SMTP (Ausgang)	25 bis25	X		192.168.1.102	X
POP3 (Eingang)	110 bis 110	X		192.168.1.102	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internet-Anwendungen verwenden.

Zum Verwenden von Online-Spielen oder Internet-Anwendungen ist i. d. R. kein Port-Forwarding oder DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internet-Anwendungen anwenden. Dafür müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internet-Anwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internet-Anwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

Benutzerdefinierte Anwendung	Externer Anschluss	TCP	UDP	IP-Adresse	Aktivieren
UT	7777 bis 27900	X	X	192.168.1.100	X
Halflife	27015 bis 27015	X	X	192.168.1.105	X
PCAnywhere	5631 bis 5631		X	192.168.1.102	X
VPN/IPSEC	500 bis 500		X	192.168.1.100	X

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

8. Weder Internetspiel, Internetserver noch Internetanwendung funktionieren.

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ (*DeMilitarized Zone*)-Hosting mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Weiterleitungseinträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da das Forwarding Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: In dem Gateway eingehende Daten werden zuerst nach den Forwarding-Einstellungen überprüft. Falls die Daten von einer Portnummer eingehen, für die kein Port-Forwarding aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)

- Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (Aktiviert) aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zum Port-Forwarding, und deaktivieren bzw. entfernen Sie die Einträge zum Forwarding. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

9. Ich habe das Kennwort vergessen bzw. die Aufforderung zur Eingabe des Kennworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.

- Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Kennworts aufgefordert werden, führen Sie die folgenden Schritte aus:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardkennwort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
  2. Geben Sie in das Feld für das Gateway-Kennwort ein anderes Kennwort ein. Geben Sie anschließend das gleiche Kennwort in das zweite Feld ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

10. Wie kann ich als PPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?

Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da das Gateway das Gateway für die Internetverbindung ist, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Netscape 4.7 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorne zu beginnen.

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Kennwort, die Forwarding-Funktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway greift auf die werkseitigen Konfigurationseinstellungen zurück.

12. Ich möchte die Firmware aktualisieren.

Um die aktuellsten Funktionen für Ihre Firmware zu erhalten, gehen Sie auf die internationale Website von Linksys und laden Sie die neueste Firmware unter www.linksys.com/international herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Products** (Produkte), und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Webseite des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.
  4. Um die Firmware zu aktualisieren, führen Sie die in „Kapitel 5: Konfigurieren des Gateways“ im Abschnitt **Administration** (Verwaltung) aufgeführten Schritte durch.

13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.
- Legen Sie auf dem Computer eine statische IP-Adresse fest. Folgen Sie dazu den Anweisungen unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“. Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder der Registerkarte **Administration** (Verwaltung) im webbasierten Dienstprogramm des Gateways vor.

14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Setup-Option zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.

1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Kennwort ein. (Der Standardbenutzername und das Standardkennwort sind **admin**.)
3. Wählen Sie im Setup-Fenster die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest.
4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status** (Status), und klicken Sie auf Schaltfläche **Connect** (Verbinden).
5. Möglicherweise wird für den Anmeldestatus **Connecting** (Verbindung wird hergestellt) angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Connected** (Verbunden) für den Anmeldestatus angezeigt wird.
6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.

- Falls die Verbindung erneut unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung wiederherzustellen.

15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich bekomme nur beschädigte Daten aus dem Internet.

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*, Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Kennwort ein. (Der Standardbenutzername und das Standardkennwort sind **admin**.)
  3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert 1492 ein.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Wenn Sie weiterhin Schwierigkeiten erfahren haben, ändern Sie den MTU-Wert auf einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis Ihr Problem gelöst ist:
  1462
  1400
  1362
  1300

16. Die Netzstrom-LED leuchtet durchgehend.

Die Netzstrom-LED leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Zwischenzeitlich fährt der Computer hoch und wird auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED immer noch blinkt, funktioniert das Gerät nicht ordnungsgemäß. Führen Sie einen Firmware-Flash durch, indem Sie dem Computer eine statische IP-Adresse zuweisen, und aktualisieren Sie anschließend die Firmware. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse 192.168.1.50, Subnetzmaske 255.255.255.0.

17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang nochmals auszuführen.

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standardgateway und DNS). Starten Sie den Computer, bei dem das Problem aufgetreten ist, erneut.

- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, dass es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Gateway her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/DSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.
- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.
- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Häufig gestellte Fragen

Wie viele IP-Adressen kann das Gateway maximal unterstützen?
Das Gateway unterstützt bis zu 253 IP-Adressen.

Unterstützt das Gateway IPSec-Passthrough?
Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

An welcher Stelle im Netzwerk wird das Gateway installiert?
In einer typischen Umgebung wird das Gateway zwischen der ADSL-Wandbuchse und dem LAN installiert.

Unterstützt das Gateway IPX oder AppleTalk?
Nein. TCP/IP ist der einzige Internet-Protokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets an ein LAN verwendet werden.

Unterstützt die LAN-Verbindung des Gateways 100-MBit/s-Ethernet?
Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 MBit/s.

Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?
Die Netzwerk-Adressen-Übersetzung (*Network Address Translation*, NAT) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheitsstufe erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private Adressen hinter einer einzigen vom ISP zur Verfügung gestellten Adresse verwenden.

Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?
Ja. Linksys bietet jedoch derzeit keinen technischen Kundendienst hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als für die Windows-Betriebssysteme an.

Unterstützt das Gateway die ICQ-Dateiübertragung?
Ja, mithilfe der folgenden Lösung: Klicken Sie auf das Menü **ICQ**, **Preference** (Einstellungen) und auf die Registerkarte **Connections** (Verbindungen), und aktivieren Sie die Option **I am behind a firewall or proxy** (Ich bin hinter einer Firewall oder einem Proxy). Legen Sie nun in den Einstellungen für die Firewall für die Zeitüberschreitung 80 Sekunden fest. Ein Internetbenutzer kann nun eine Datei an einen Benutzer hinter dem Gateway senden.

Ich kann einen Unreal Tournament-Server einrichten, andere Benutzer im LAN können sich jedoch nicht mit dem Server verbinden. Was muss ich tun?
Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN sowie die Weiterleitungs-Ports 7777, 7778, 7779, 7780, 7781 und 27900 für die IP-Adresse des Servers einrichten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie die Weiterleitung an einen weiteren Port vornehmen. (Die Einstellung „Port 8080“ kann hier eingesetzt werden, findet jedoch nur bei einer Remote-Administration Verwendung. Sie müssen u. U. diese Funktion deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für „ListenPort“ den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für „ServerName“ die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?
Das hängt vom verwendeten Netzwerkspiel bzw. vom verwendeten Server ab. So unterstützt z. B. Unreal Tournament eine mehrfache Anmeldung bei nur einer öffentlichen IP-Adresse.

Wie kann ich Half-Life - Team Fortress mit dem Gateway verwenden?
Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen „+clientport 2700x“ hinzugefügt werden, wobei x dann 6, 7, 8 usw. entspricht. Dadurch können sich mehrere Computer mit dem gleichen Server verbinden. Problem: Bei Version 1.0.1.6 können mehrere Computer, die die gleiche CD-Kennnummer verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Ausführen von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

Die Webseite reagiert nicht, heruntergeladene Dateien sind beschädigt oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?
Legen Sie für Ihren Ethernet-Adapter 10 MBit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Aushandlung. (Rufen Sie über die Netzwerksystemsteuerung die Registerkarte für die erweiterten Eigenschaften des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste drücken, bis die Netzstrom-LED aufleuchtet und wieder erlischt. Setzen Sie das DSL-Modem zurück, indem Sie die Einheit aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?
Sämtliche Aktualisierungen für Linksys-Firmware werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **System** des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

Funktioniert das Gateway in einer Macintosh-Umgebung?
Ja, es kann jedoch nur über Internet Explorer 4.0 bzw. über Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugegriffen werden.

Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

Was bedeutet DMZ-Hosting?
Mithilfe der DMZ (*Demilitarized Zone*, entmilitarisierte Zone) kann über eine IP-Adresse (d. h. einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in „Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Verwenden bei DMZ-Hosting sowohl Benutzer als auch Gateway die öffentliche IP-Adresse?
Nein.

Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

Ist das Gateway auch plattformübergreifend einsetzbar?
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

Wie viele Ports können gleichzeitig weitergeleitet werden?
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

Über welche erweiterten Funktionen verfügt das Gateway?
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Forwarding, Routing und DDNS.

Wie viele VPN-Sitzungen unterstützt das Gateway maximal?
Die maximale Anzahl hängt von vielen Faktoren ab. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen; je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.

Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?
Wenden Sie sich für diese Informationen an Ihren ISP.

Wie kann ich mIRC mit dem Gateway verwenden?
Legen Sie in der Registerkarte **Port Forwarding** (Port-Weiterleitung) den Wert 113 für den Computer fest, auf dem Sie mIRC verwenden möchten.

Kann das Gateway als DHCP-Server eingesetzt werden?
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

Kann ich eine Anwendung von einem standortfernen Computer aus über das Wireless-Netzwerk ausführen?
Dies ist abhängig davon, ob die Anwendung zur Verwendung in einem Netzwerk entwickelt wurde. Weitere Informationen dazu, ob die Anwendung in einem Netzwerk verwendet werden kann, finden Sie in der Dokumentation zur Anwendung.

Was ist der IEEE 802.11g-Standard?
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, jedoch nur unter der Voraussetzung, dass die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?
Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Kanal-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Paketauftrennung
- Energieverwaltung

Was bedeutet Ad-Hoc-Modus?
Wenn für ein Wireless-Netzwerk der Ad-Hoc-Modus festgelegt ist, sind die Wireless-fähigen Computer so konfiguriert, dass sie ohne Zugriffspunkt direkt miteinander kommunizieren (Peer-to-Peer).

Was bedeutet Infrastrukturmodus?
Ist für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt, ist es so konfiguriert, dass es mit einem Netzwerk über einen drahtlosen Zugriffspunkt kommuniziert.

Was ist Roaming?
Roaming bezeichnet die Möglichkeit, bei Verwendung von tragbaren Computern kontinuierlich über eine größere Distanz hinweg zu kommunizieren, als durch einen einzigen Zugriffspunkt abgedeckt werden kann. Vor Verwendung des Roaming muss der Computer auf die gleiche Kanalnummer wie der Zugriffspunkt des dedizierte Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das drahtlose LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Zugriffspunkt bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Um diese Funktionen gleichzeitig verwenden zu können, ist eine dynamische Netzwerktechnologie erforderlich, durch die Zugriffspunkte und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Zugriffspunkt verarbeitet wird, und die Entfernung zwischen jedem Zugriffspunkt zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Zugriffspunkt und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem Original-Zugriffspunkt vorliegt oder ob ein neuer Zugriffspunkt gesucht werden soll. Wenn ein Knoten keine Bestätigung des Original-Zugriffspunkts mehr erhält, wird eine neue Verbindungssuche gestartet. Wenn ein neuer Zugriffspunkt gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

Was bedeutet ISM-Band?

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High-Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

Was bedeutet Bandspreizung?

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*, Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*, Frequenzsprungverfahren).

Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

Können die Daten bei der Funkübertragung abgefangen werden?
WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*; direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

Was ist WEP?
WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

Was ist eine MAC-Adresse?
Eine MAC (*Media Access Control*)-Adresse ist eine eindeutige Nummer, die vom Hersteller jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

Wie setze ich das Gateway zurück?
Halten Sie die Reset-Taste auf der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

Wie behebe ich einen Signalverlust?
Ohne Überprüfung ist es nicht möglich, den genauen Bereich Ihres Wireless-Netzwerks zu bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer und stellen Sie beide Geräte schrittweise weiter entfernt auf, um dadurch die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da dies Störungen, die nur einen Kanal betreffen, vermindert.

Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.
WEP ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass die gleichen WEP-Schlüssel und -Ebenen (64 bzw. 128) in allen Knoten in Ihrem Wireless-Netzwerk verwendet werden.

Wie viele Kanäle/Frequenzen sind mit dem Gateway verfügbar?
Es stehen insgesamt 11 Kanäle, von 1 bis 11 (für Nordamerika), zur Verfügung.

Falls Sie hier keine Antworten auf Ihre Fragen erhalten haben, finden Sie weitere Informationen auf der internationalen Website von Linksys unter http://www.linksys.com/international.

Anhang B: Sicherheit im Wireless-Netzwerkbetrieb

Wichtige Informationen für drahtlose Produkte

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres drahtlosen Netzwerks.

1. Leistung:

Die Leistung Ihres drahtlosen Netzwerks hängt von einer Reihe von Faktoren ab:

Die Entfernung vom Zugriffspunkt in einer Infrastrukturumgebung. Je weiter Sie entfernt sind, desto geringer wird die Übertragungsgeschwindigkeit.

Strukturelle Interferenzen: Die bauliche Auslegung bzw. Struktur Ihres Gebäudes sowie die Bauart und die Baumaterialien wirken sich unter Umständen negativ auf die Signalqualität und -geschwindigkeit aus.

Der Standort und die Ausrichtung der drahtlosen Geräte.

2. Interferenzen:

Jedes Gerät, das innerhalb des 2,4-GHz-Spektrums arbeitet, kann Netzwerkinterferenzen bei drahtlosen 802.11b- oder 802.11g-Geräten verursachen. Störungen können unter anderem von schnurlosen 2,4-GHz-Telefonen, Mikrowellenöfen, sich in der Nähe befindlichen öffentlichen „Hotspots“ und drahtlosen 802.11b- oder 802.11g-Wireless-LANs ausgehen.

3. Sicherheit:

Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen, die ein Eingreifen Ihrerseits erfordern, um diese umsetzen zu können.

Führen Sie von der nachfolgend aufgeführten vollständigen Liste mindestens die Schritte A bis E durch:

A. Ändern Sie die Standard-SSID.

B. Deaktivieren Sie SSID-Übertragungen.

C. Ändern Sie das Standardkennwort für das Administrator-Konto.

D. Aktivieren Sie die MAC-Adressfilterung.

E. Ändern Sie die SSID regelmäßig.

F. Aktivieren Sie die 128-Bit-WEP-Verschlüsselung. Beachten Sie, dass die Netzwerkleistung hierdurch verringert wird.

G. Ändern Sie die WEP-Verschlüsselungsschlüssel regelmäßig.

Informationen zum Umsetzen dieser Sicherheitsfunktionen finden Sie im Benutzerhandbuch.

4. Sicherheitsrisiken für Wireless-Netzwerke

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen sind entschlüsselt und enthalten umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set Identifier*) des Netzwerks und die IP-Adresse des Netzwerk-PCs oder Zugriffspunkts. Dagegen können Sie sich folgendermaßen schützen:

Ändern Sie das Administratorkennwort regelmäßig. Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorkennwort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorkennwort regelmäßig.

SSID: In Zusammenhang mit der SSID ist Folgendes zu beachten:

A. Deaktivieren Sie Übertragungen.

B. Wählen Sie eine individuelle SSID.

C. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind ab Werk auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys“.) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID zu einer individuellen Angabe, die keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr drahtloses Netzwerk verschafft haben, erneut das Kennwort knacken müssen.

MAC-Adressen: Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur drahtlosen Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es den Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

WEP-Verschlüsselung: WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel gegen Sicherheitsrisiken bei drahtlosen Geräten gesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es dem Hacker das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

A. Verwenden Sie die höchste Verschlüsselungsebene.

B. Verwenden Sie einen freigegebenen Schlüssel.

C. Verwenden Sie mehrere WEP-Schlüssel.

D. Ändern Sie Ihre WEP-Schlüssel regelmäßig.

Verschlüsselungsfunktionen haben negative Auswirkungen auf die Netzwerkleistung. Wenn Sie sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Durch die Einhaltung dieser Sicherheitsempfehlungen können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos nutzen.

Anhang C: Konfigurieren von IPSec zwischen einem Windows 2000/XP-Computer und dem Gateway

Einführung

In diesem Dokument finden Sie Anweisungen dazu, wie Sie über vorläufige gemeinsame Schlüssel einen sicheren IPSec-Tunnel einrichten, um ein privates Netzwerk innerhalb des VPN-Gateways mit einem Windows 2000- oder Windows XP-Computer zu verbinden. Detaillierte Informationen zur Konfiguration von Windows 2000-Servern finden Sie auf der Website von Microsoft:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

HINWEIS: Zeichnen und bewahren Sie sämtliche von Ihnen vorgenommenen Änderungen auf. Diese Änderungen sind für die Windows-Anwendung „secpol“ und dem webbasierten Dienstprogramm des Routers identisch.

Umgebung

Die hier erwähnten IP-Adressen und weiteren Einstellungen sind lediglich zu Darstellungszwecken aufgeführt.

Für Windows 2000 oder XP:
IP-Adresse: 140.111.1.2 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0

WAG54G

WAN-IP-Adresse: 140.111.1.1 <= Die IP-Adresse wird vom ISP des Benutzers zur Verfügung gestellt; die hier aufgeführte WAN-IP-Adresse dient lediglich als Beispiel.

Subnetzmaske: 255.255.255.0
LAN-IP-Adresse: 192.168.1.1
Subnetzmaske: 255.255.255.0

HINWEIS: Die Anweisungen und Abbildungen in diesem Abschnitt der Anleitung beziehen sich auf den Router. Ersetzen Sie „Gateway“ durch „Router“. Die Optionen „OK“ bzw. „Schließen“ können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Hinweise zum Einrichten eines sicheren IPSecTunnels

Schritt 1: Erstellen einer IPSec-Richtlinie

1. Klicken Sie auf die Schaltfläche **Start**, wählen Sie **Ausführen** aus, und geben Sie in das Feld **Öffnen** den Eintrag **secpol.msc** ein. Das in Abbildung C-1 dargestellte Fenster **Lokale Sicherheitseinstellungen** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Lokaler Computer** (Win XP) bzw. auf **IP-Sicherheitsrichtlinien auf lokalem Computer** (Win 2000), und wählen Sie anschließend **IP-Sicherheitsrichtlinie erstellen** aus.
3. Klicken Sie auf die Schaltfläche **Weiter**, und geben Sie für Ihre Richtlinie einen Namen ein (zum Beispiel „an_Router“). Klicken Sie anschließend auf **Weiter**.
4. Deaktivieren Sie das Kontrollkästchen **Die Standardantwortregel aktivieren**, und klicken Sie anschließend auf die Schaltfläche **Weiter**.
5. Klicken Sie auf die Schaltfläche **Fertig stellen**, und vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert ist.

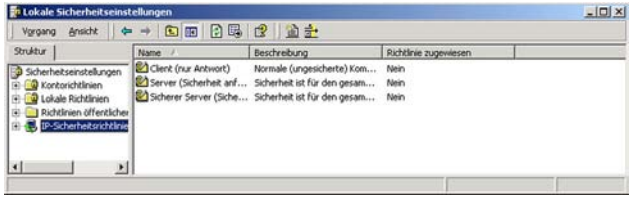

Abbildung C-1: Fenster „Lokale Sicherheitseinstellungen“

HINWEIS: Jeder Bezug in diesem Kapitel auf „win” verweist auf Windows 2000 und Windows XP. Ersetzen Sie die Hinweise auf „Router“ mit „Gateway“. Die Optionen „OK“ bzw. „Schließen“ können in den auf Ihrem Computer angezeigten Fenstern vom Text in der Anleitung abweichen; klicken Sie auf die Ihrem Fenster entsprechende Schaltfläche.

Schritt 2: Erstellen von Filterlisten

Filterliste 1: win->Router

1. Vergewissern Sie sich, dass im Fenster für die Eigenschaften der neuen Richtlinie die Registerkarte **Regeln** ausgewählt ist (siehe Abbildung C-2). Deaktivieren Sie das Kontrollkästchen **Assistent verwenden**, und klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel zu erstellen
2. Stellen Sie sicher, dass die Registerkarte **IP-Filterliste** ausgewählt ist, und klicken Sie auf die Schaltfläche **Hinzufügen** (siehe Abbildung C-3). Das Fenster **IP-Filterliste** wird angezeigt (siehe Abbildung C-4). Geben Sie für die Filterliste einen geeigneten Namen, wie z. B. win->Router, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

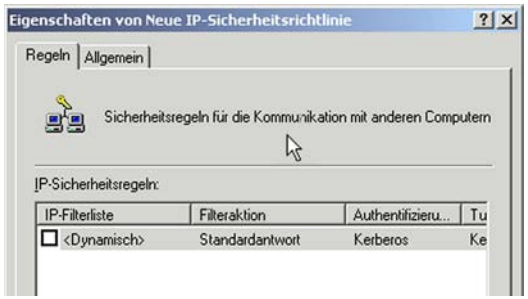

Abbildung C-2: Registerkarte „Regeln“

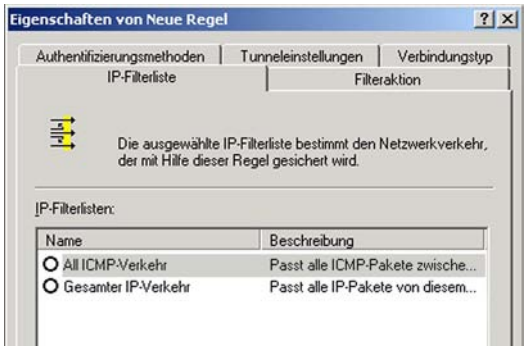

Abbildung C-3: Registerkarte „IP-Filterliste“

3. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung C-5). Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Eigene IP-Adresse** aus. Wählen Sie im Feld **Zieladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Dabei handelt es sich um die Standardeinstellungen des Routers. Falls Sie an diesen Einstellungen Änderungen vorgenommen haben, geben Sie die geänderten Werte ein.)

4. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

5. Klicken Sie auf **OK**. Klicken Sie anschließend im Fenster **Filterliste** auf die Schaltfläche **OK** bzw. **Schließen**.

Filterliste 2: Router ->win

6. Das Fenster **Eigenschaften von neue Regel** wird angezeigt (siehe Abbildung C-6). Wählen Sie die Registerkarte **IP-Filterliste** aus, und stellen Sie sicher, dass **win -> Router** markiert ist. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

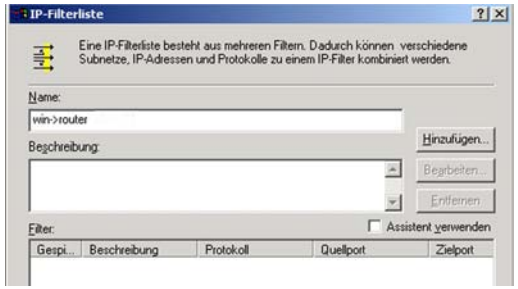

Abbildung C-4: Dialogfeld „IP-Filterliste“

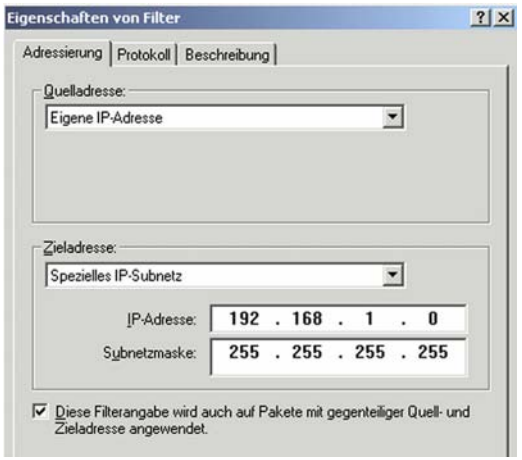

Abbildung C-5: Dialogfeld „Eigenschaften von Filter“

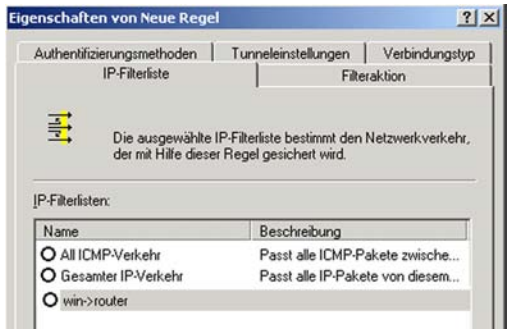

Abbildung C-6: Eigenschaften von Neue Regel

7. Das Fenster **IP-Filterliste** wird angezeigt (siehe Abbildung C-7). Geben Sie für die Filterliste einen geeigneten Namen, wie z. B. Router -> win, ein, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

8. Das Fenster für die Filtereigenschaften wird angezeigt (siehe Abbildung C-8). Wählen Sie die Registerkarte **Adressierung**. Wählen Sie im Feld **Quelladresse** die Option **Spezielles IP-Subnetz** aus, und geben Sie die IP-Adresse 192.168.1.0 und Subnetzmaske 255.255.255.0 ein. (Falls Sie an diesen Standardeinstellungen Änderungen vorgenommen haben, geben Sie hier die neuen Werte ein.) Wählen Sie im Feld **Zieladresse** die Option **Eigene IP-Adresse** aus.

9. Wenn Sie eine Beschreibung für Ihren Filter eingeben möchten, klicken Sie auf die Registerkarte **Beschreibung** und geben die Beschreibung ein.

10. Klicken Sie auf die Schaltfläche **OK** bzw. **Schließen**, woraufhin das Fenster **Eigenschaften von Neue Regel** angezeigt wird und die Registerkarte **IP-Filterliste** ausgewählt ist (siehe Abbildung C-9). Hier sollte der Listeneintrag „Router -> win“ und „win -> Router“ aufgeführt sein. Klicken Sie im Fenster **IP-Filterliste** auf die Schaltfläche **OK** (unter Windows XP) bzw. die Schaltfläche **Schließen** (unter Windows 2000).

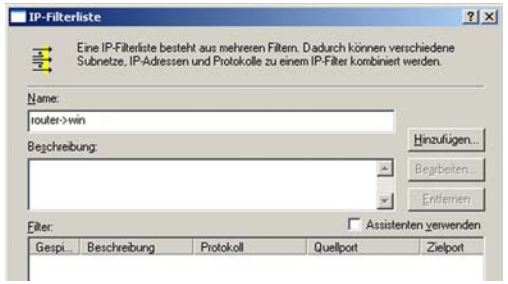

Abbildung C-7: Dialogfeld „IP-Filterliste“

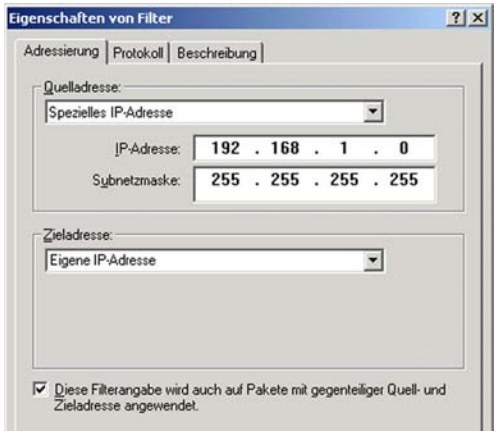

Abbildung C-8: Dialogfeld „Eigenschaften von Filter“

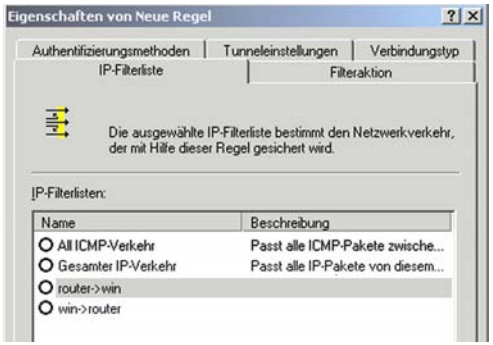

Abbildung C-9: Eigenschaften von Neue Regel

Schritt 3: Konfigurieren von individuellen Tunnelregeln

Tunnel 1: win -> Router

1. Klicken Sie, wie in Abbildung C-10 dargestellt, auf die Registerkarte **IP-Filterliste** und anschließend auf die Filterliste „win -> Router“.

2. Klicken Sie auf die Registerkarte **Filteraktion** (siehe Abbildung C-11), und klicken Sie auf die für die Filteraktion erforderliche Optionsschaltfläche **Sicherheit erforderlich**. Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

3. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung C-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikat. annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

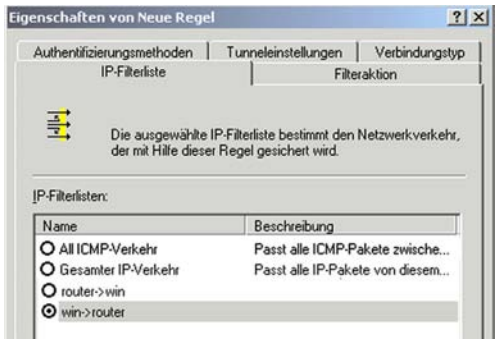

Abbildung C-10: Registerkarte „IP-Filterliste“

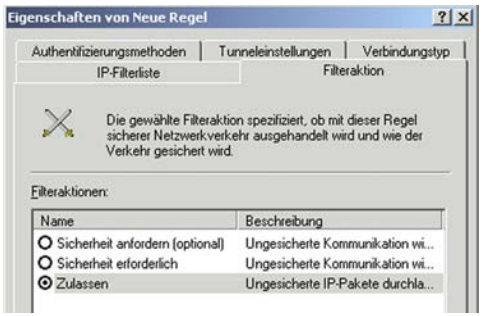

Abbildung C-11: Registerkarte „Filteraktion“

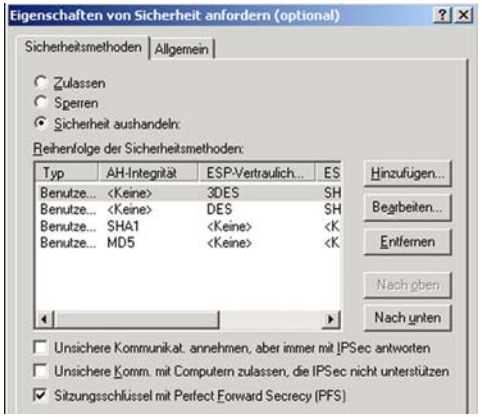

Abbildung C-12: Registerkarte „Sicherheitsmethoden“

4. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden** (siehe Abbildung C-13), und klicken Sie auf die Schaltfläche **Bearbeiten**.

5. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden** (siehe Abbildung C-14), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. Klicken Sie auf **OK**.

6. Dieser neue vorinstallierte Schlüssel ist in Abbildung C-15 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

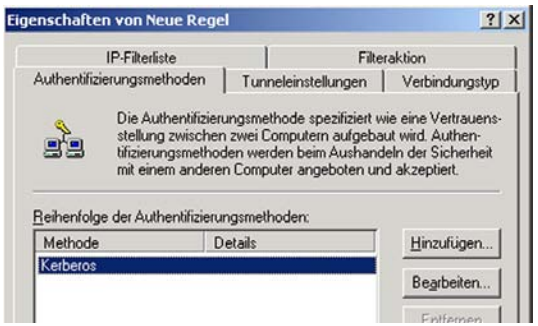

Abbildung C-13: Registerkarte „Authentifizierungsmethoden“

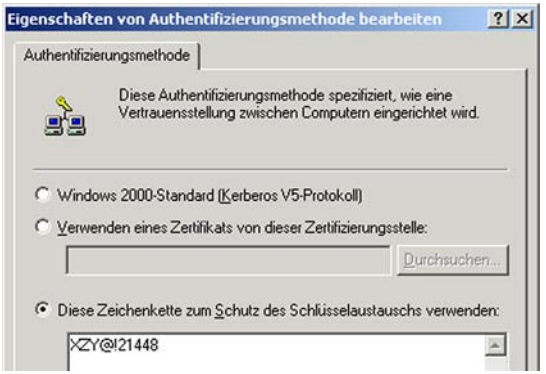
Eigenschaften von Authentifizierungsmethode bearbeiten
Authentifizierungsmethode
Diese Authentifizierungsmethode spezifiziert, wie eine Vertrauensstellung zwischen Computern eingerichtet wird.
Windows 2000-Standard (Kerberos V5-Protokoll)
Verwenden eines Zertifikats von dieser Zertifizierungsstelle:
Durchsuchen...
Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden:
XZY@!21448

Abbildung C-14: Vorinstallierter Schlüssel

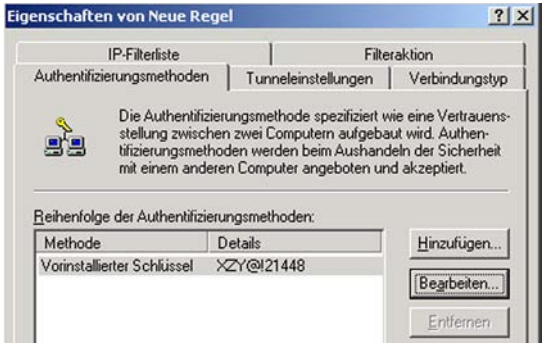

Abbildung C-15: Neuer vorinstallierter Schlüssel

7. Wählen Sie die Registerkarte **Tunneleinstellungen** (siehe Abbildung C-16), und aktivieren Sie die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**. Geben Sie anschließend die WAN-IP-Adresse des Routers ein.

8. Wählen Sie die Registerkarte **Verbindungstyp** (siehe Abbildung C-17), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um diese Regel abzuschließen.

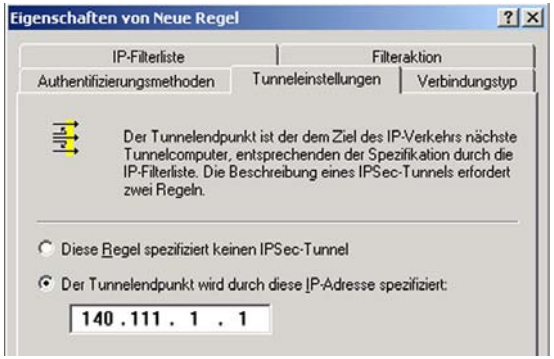
Eigenschaften von Neue Regel
IP-Filterliste
Filteraktion
Authentifizierungsmethoden
Tunneleinstellungen
Verbindungstyp
Der Tunnelendpunkt ist der dem Ziel des IP-Verkehrs nächste Tunnelcomputer, entsprechenden der Spezifikation durch die IP-Filterliste. Die Beschreibung eines IPSec-Tunnels erfordert zwei Regeln.
Diese Regel spezifiziert keinen IPSec-Tunnel
Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert:
140 . 111 . 1 . 1

Abbildung C-16: Registerkarte „Tunneleinstellungen“

Tunnel 2: Router -> win

9. Vergewissern Sie sich, dass im Dialogfeld für die Eigenschaften der neuen Richtlinie (siehe Abbildung C-18), der Eintrag „win -> Router“ ausgewählt ist, und deaktivieren Sie das Kontrollkästchen **Assistent verwenden**. Klicken Sie anschließend die Schaltfläche **Hinzufügen**, um einen zweiten IP-Filter zu erstellen.

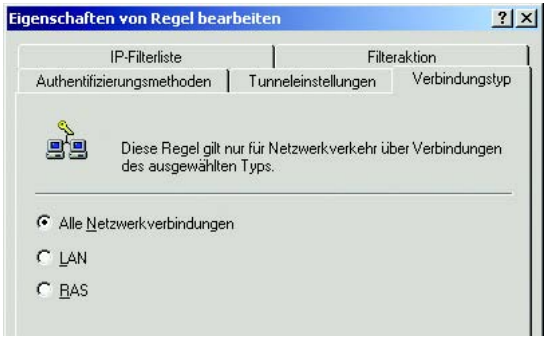

Abbildung C-17: Registerkarte „Verbindungstyp“

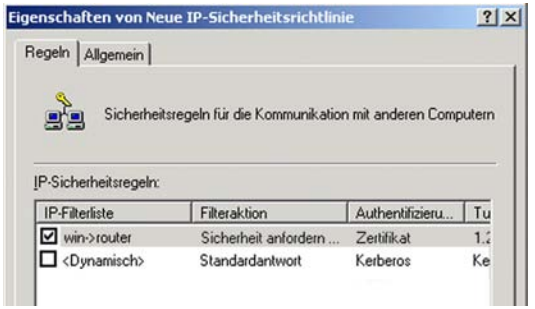

Abbildung C-18: Fenster für die Eigenschaften der neuen Richtlinie

10. Aktivieren Sie in der Registerkarte **IP-Filterliste** die Optionsschaltfläche für die Filterliste **Router -> win** (siehe Abbildung C-19).

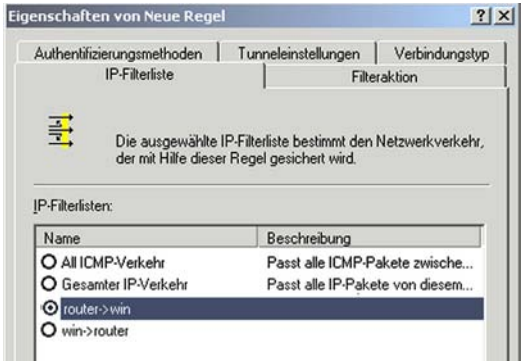

Abbildung C-19: Registerkarte „IP-Filterliste“

11. Klicken Sie auf die Registerkarte **Filteraktion**, und wählen Sie die Filteraktion **Sicherheit erforderlich** aus (siehe Abbildung C-20). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**. Stellen Sie in der Registerkarte **Sicherheitsmethoden** (siehe Abbildung C-12) sicher, dass die Option **Sicherheit aushandeln** aktiviert ist, und deaktivieren Sie das Kontrollkästchen **Unsichere Kommunikation annehmen, aber immer mit IPSec antworten**. Wählen Sie die Option **Sitzungsschlüssel mit Perfect Forward Secrecy (PFS)** aus, und klicken Sie auf die Schaltfläche **OK**.

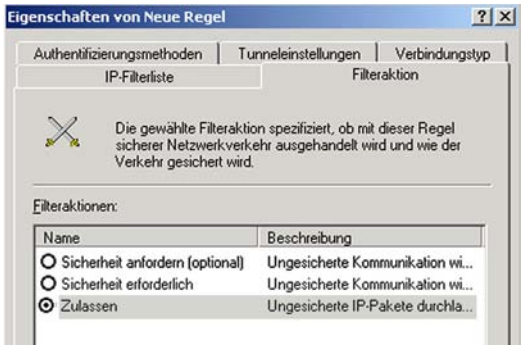

Abbildung C-20: Registerkarte „Filteraktion“

12. Klicken Sie auf die Registerkarte **Authentifizierungsmethoden**, und stellen Sie sicher, dass die Kerberos-Authentifizierungsmethode aktiviert ist (siehe Abbildung C-21). Klicken Sie anschließend auf die Schaltfläche **Bearbeiten**.

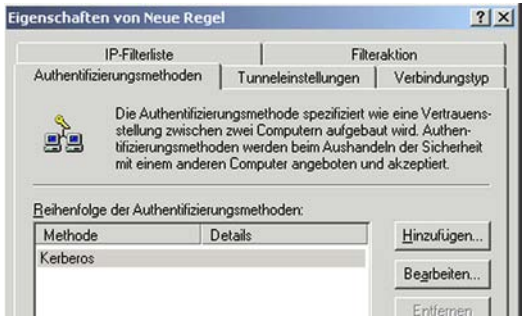

Abbildung C-21: Registerkarte „Authentifizierungsmethode“

13. Ändern Sie die Authentifizierungsmethode auf **Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden** (siehe Abbildung C-22), und geben Sie die Zeichenkette für den vorinstallierten Schlüssel, z. B. XYZ12345, ein. (Die hier aufgeführte Schlüsselzeichenkette dient als Beispiel. Ihre Schlüsselzeichenkette sollte eindeutig und leicht zu merken sein.) Klicken Sie anschließend auf die Schaltfläche **OK**.

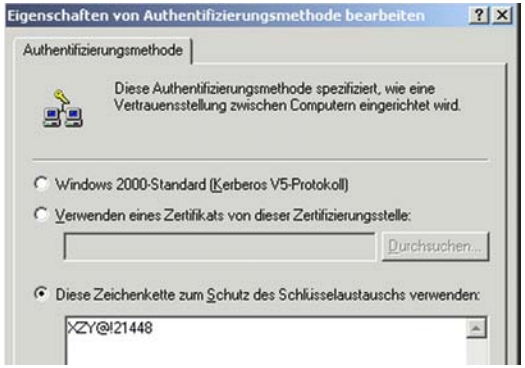
Eigenschaften von Authentifizierungsmethode bearbeiten
Authentifizierungsmethode
Diese Authentifizierungsmethode spezifiziert, wie eine Vertrauensstellung zwischen Computern eingerichtet wird.
Windows 2000-Standard (Kerberos V5-Protokoll)
Verwenden eines Zertifikats von dieser Zertifizierungsstelle:
Durchsuchen...
Diese Zeichenkette zum Schutz des Schlüsselaustauschs verwenden:
XZY@!21448

Abbildung C-22: Vorinstallierter Schlüssel

14. Dieser neue vorinstallierte Schlüssel ist in Abbildung C-23 aufgeführt. Klicken Sie gegebenenfalls auf die Schaltfläche **Übernehmen**, um fortzufahren; andernfalls fahren Sie mit dem nächsten Schritt fort.

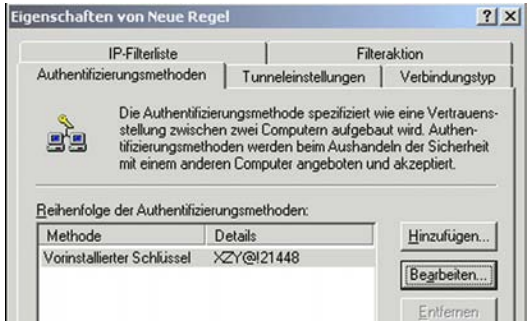

Abbildung C-23: Neuer vorinstallierter Schlüssel

15. Aktivieren Sie in der Registerkarte **Tunneleinstellungen** (siehe Abbildung C-24) die Optionsschaltfläche **Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert**, und geben Sie die IP-Adresse des Computers ein, auf dem Windows 2000 bzw. Windows XP verwendet wird.

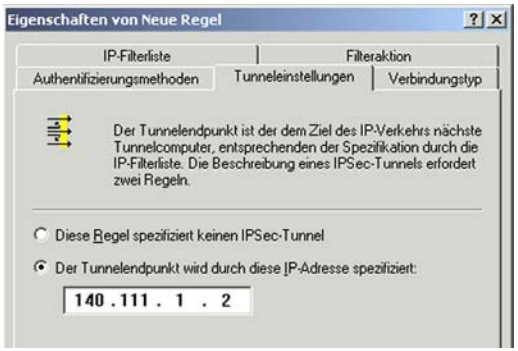
Eigenschaften von Neue Regel
IP-Filterliste
Filteraktion
Authentifizierungsmethoden
Tunneleinstellungen
Verbindungstyp
Der Tunnelendpunkt ist der dem Ziel des IP-Verkehrs nächste Tunnelcomputer, entsprechenden der Spezifikation durch die IP-Filterliste. Die Beschreibung eines IPSec-Tunnels erfordert zwei Regeln.
Diese Regel spezifiziert keinen IPSec-Tunnel
Der Tunnelendpunkt wird durch diese IP-Adresse spezifiziert:
140 . 111 . 1 . 2

Abbildung C-24: Registerkarte „Tunneleinstellungen“

16. Klicken Sie auf die Registerkarte **Verbindungstyp** (siehe Abbildung C-25), und klicken Sie auf **Alle Netzwerkverbindungen**. Klicken Sie anschließend auf die Schaltfläche **OK** bzw. auf **Schließen**, um den Vorgang zu beenden.

17. Klicken Sie in der Registerkarte **Regeln** (siehe Abbildung C-26) auf die Schaltfläche **OK** bzw. auf **Schließen**, um zum secpol-Bildschirm zurückzukehren.

Abbildung C-25: Verbindungstyp

Schritt 4: Zuweisen einer neuen IPSec-Richtlinie

Klicken Sie mit der rechten Maustaste auf den Eintrag **IP-Sicherheitsrichtlinien auf lokalem Computer** (Abbildung C-27) und anschließend mit der rechten Maustaste auf die Richtlinie „an_Router“. Klicken Sie nun auf die Option **Zuweisen**. Im Ordnersymbol wird ein grüner Pfeil angezeigt.

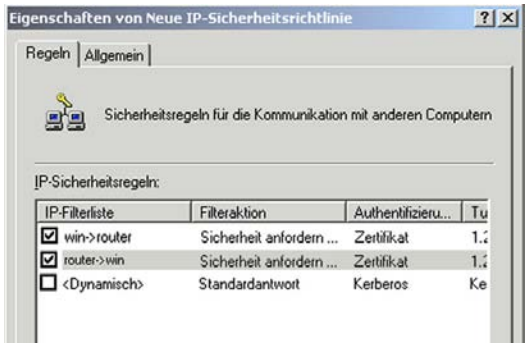

Abbildung C-26: Regeln

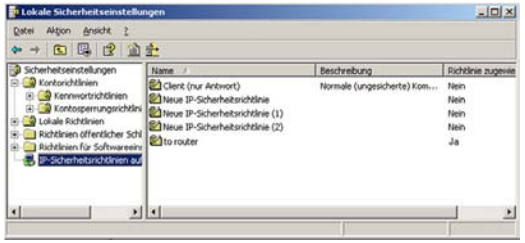

Abbildung C-27: Lokaler Computer

Schritt 5: Erstellen eines Tunnels mithilfe des webbasierten Dienstprogramms

1. Geben Sie im Adressfeld des Browsers **192.168.1.1** ein. Drücken Sie die Eingabetaste.
2. Wenn die Felder **Benutzername** und **Kennwort** angezeigt werden, geben Sie den Standard-Benutzernamen und das -Kennwort **admin** ein. Drücken Sie die Eingabetaste.
3. Klicken Sie in der Registerkarte **Setup** (Einrichtung) auf die Registerkarte **VPN**.
4. Wählen Sie in der Registerkarte **VPN**, wie in Abbildung C-28 dargestellt, den zu erstellenden Tunnel aus der Dropdown-Liste **Select Tunnel Entry** (Tunneleintrag auswählen) aus. Klicken Sie dann auf **Enabled** (Aktiviert). Geben Sie im Feld **Tunnel Name** (Tunnelname) den Namen des Tunnels ein. Auf diese Weise können Sie die verschiedenen Tunnel erkennen. Der eingegebene Name muss nicht dem Namen entsprechen, der am anderen Ende des Tunnels verwendet wird.
5. Geben Sie im Feld **Local Secure Group** (Lokale sichere Gruppe) die IP-Adresse und Subnetzmaske des lokalen VPN-Routers ein. Geben für den letzten IP-Adressensatz 0 ein, um das gesamte IP-Subnetz freizugeben (z. B. 192.168.1.0).
6. Geben Sie im Feld **Remote Security Gateway** (Entferntes Sicherheits-Gateway) die IP-Adresse und die Subnetzmaske des VPN-Geräts am anderen Ende des Tunnels ein (der entfernte VPN-Router oder das Gerät, mit dem Sie kommunizieren möchten).
7. Wählen Sie aus zwei unterschiedlichen Verschlüsselungstypen aus: **DES** oder **3DES** (empfohlen wird **3DES**, weil dieser Typ sicherer ist). Sie können einen der beiden Typen wählen; die Einstellung muss jedoch mit dem Verschlüsselungstyp übereinstimmen, der vom VPN-Gerät am anderen Ende des Tunnels verwendet wird. Sie können aber auch ohne Verschlüsselung arbeiten, indem Sie **Disable** (Deaktivieren) auswählen.
8. Wählen Sie aus zwei Authentifizierungstypen aus: **MD5** und **SHA** (empfohlen wird **SHA**, weil dieser Typ sicherer ist). Wie bei der Verschlüsselung kann einer der beiden Typen gewählt werden, vorausgesetzt, das VPN-Gerät am anderen Ende des Tunnels verwendet denselben Authentifizierungstyp. Die Authentifizierung kann aber auch mit **Disable** (Deaktivieren) an beiden Enden des Tunnels deaktiviert werden.
9. Wählen Sie die Schlüsselverwaltung aus. Wählen Sie **Auto (IKE)**, und geben Sie eine Reihe von Zahlen oder Buchstaben in das Feld **Pre-shared Key** (Vorläufiger gemeinsamer Schlüssel) ein. Markieren Sie das Kontrollkästchen neben **PFS (Perfect Forward Secrecy)** [Vollständige Geheimhaltung bei Weiterleitung], um sicherzustellen, dass der erste Schlüsselaustausch und die IKE-Vorschläge sicher sind. Sie können in diesem Feld eine Kombination aus bis zu 24 Zahlen und Buchstaben eingeben. Es dürfen keine Sonderzeichen oder Leerzeichen verwendet werden. Im Feld **Key Lifetime** (Schlüssel-Verwendungsdauer) können Sie die Gültigkeitsdauer eines Schlüssels festlegen. Geben Sie die gewünschte Nutzungszeit in Sekunden ein, oder lassen Sie das Feld leer, so dass der Schlüssel unbegrenzt lange zur Verfügung steht.
10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu speichern.

Der Tunnel ist nun hergestellt.

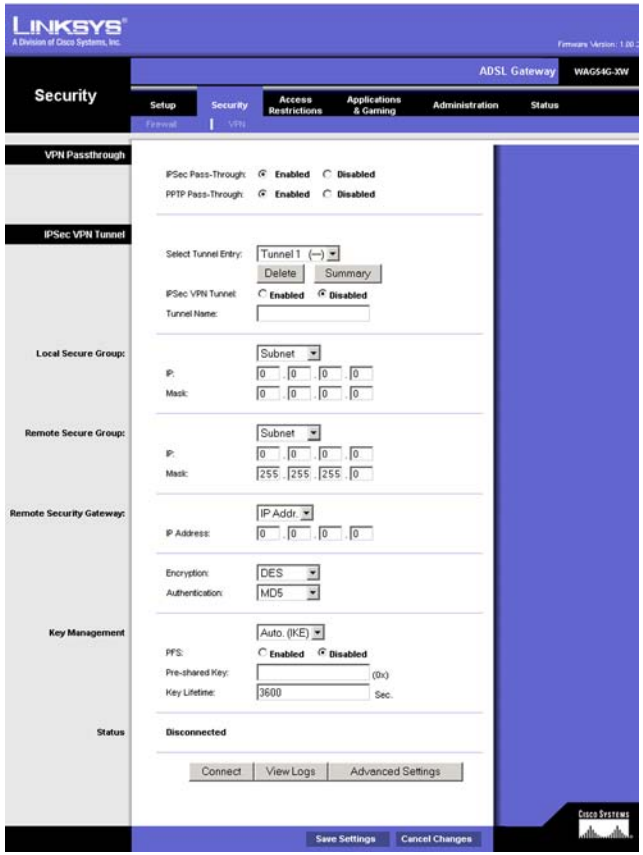

Abbildung C-28: Registerkarte „VPN“

Anhang D: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Weiterleitungs- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen winipcfg** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster **IP-Konfiguration** den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung D-1.

3. Notieren Sie die Adapteradresse so, wie sie auf dem Bildschirm Ihres Computers angezeigt wird (siehe Abbildung D-2). Sie bildet die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung D-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung D-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

Hinweis: Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

Abbildung D-1: Fenster „IP-Konfiguration“

Abbildung D-2: MAC-Adresse/Adapteradresse

Anweisung für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Hinweis: Die MAC-Adresse wird auch als physikalische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **ipconfig /all** ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physikalische Adresse so, wie sie am Computer anzeigt wird (Abbildung D-3). Diese Adresse stellt die MAC-Adresse Ihres Ethernet-Adapters dar. Sie wird als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/physikalische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung D-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf Ihrem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung E-1 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf Ihrem Computer angezeigte Adresse kann davon abweichen.

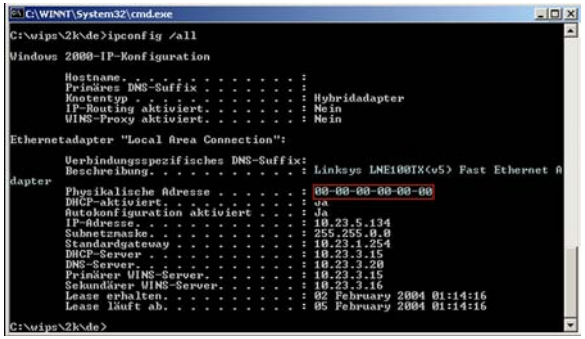
C:\WINNT\System32\cmd.exe
C:\wips\2k\de>ipconfig /all
Windows 2000-IP-Konfiguration
Hostname . . . . . :
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybridadapter
IP-Routing aktiviert. . . . . : Nein
WINS-Proxy aktiviert. . . . . : Nein
Ethernetadapter "Local Area Connection":
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
Physikalische Adresse . . . . . : 00-00-00-00-00-00
DHCP-aktiviert. . . . . : ja
Autokonfiguration aktiviert . . . : Ja
IP-Adresse. . . . . : 10.23.5.134
Subnetzmaske. . . . . : 255.255.0.0
Standardgateway . . . . . : 10.23.1.254
DHCP-Server . . . . . : 10.23.3.15
DNS-Server. . . . . : 10.23.3.28
Primärer WINS-Server. . . . . : 10.23.3.15
Sekundärer WINS-Server. . . . . : 10.23.3.16
Lease erhalten. . . . . : 02 February 2004 01:14:16
Lease läuft ab. . . . . : 05 February 2004 01:14:16
C:\wips\2k\de>_

Abbildung D-3: MAC-Adresse/physikalische Adresse

Anhang E: Aktualisieren der Firmware

Die Firmware des Gateways wird über die Registerkarte **Administration** (Verwaltung) des webbasierten Dienstprogramms aktualisiert. Führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen, die Sie von der internationalen Website von Linksys heruntergeladen und extrahiert haben. (Verwenden Sie für das Gateway keine Firmware von der US-Website.)
2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und folgen Sie den daraufhin angezeigten Anweisungen.

Abbildung E-1: Firmware aktualisieren

Anhang F: Glossar

802.11a - IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 MBit/s sowie eine Betriebsfrequenz von 5 GHz festlegt.

802.11b - IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 MBit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

802.11g - IEEE-Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 MBit/s und eine Betriebsfrequenz von 2,4 GHz festlegt sowie Abwärtskompatibilität mit Geräten garantiert, die dem Standard 802.11b entsprechen.

Access Point - Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem Kabelnetzwerk kommunizieren können. Wird auch verwendet, um die Reichweite eines Wireless-Netzwerks zu erweitern.

Adapter - Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhalten kann.

Ad-hoc (Ad-hoc-Modus) - Eine Gruppe drahtloser Geräte, die direkt miteinander kommunizieren (Peer-to-Peer) statt über einen Access Point.

Aktualisierung - Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

Backbone - Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

Bandbreite - Die Übertragungskapazität eines bestimmen Geräts oder Netzwerks.

Beacon-Intervall - Das Sendeintervall des Beacons, einer Paketübertragung eines Gateways zur Synchronisierung eines Wireless-Netzwerks.

Bit - Eine Informationseinheit.

Breitband - Eine stets aktive, schnelle Internetverbindung.

Bridge - Ein Gerät, das zwei verschiedene lokale Netzwerke verbindet, wie beispielsweise ein Wireless-Netzwerk mit einem verdrahteten Netzwerk.

Browser - Ein Browser ist eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen zugegriffen werden kann.

CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) - Eine Datenübertragungsmethode, die verwendet wird, um Datenverluste im Netzwerk zu verhindern.

CTS (*Clear To Send*) - Ein von einem Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

Daisy Chain *(Verkettung)* - Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

Datenbank - Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

DDNS (*Dynamic Domain Name System*) - System, in dem eine Website, ein FTP oder E-Mail-Server mit einer dynamischen IP-Adresse einen festen Domänennamen verwenden kann.

DHCP (*Dynamic Host Configuration Protocol*) - Ein Protokoll, das es einem Gerät in einem LAN (auch als DHCP-Server bezeichnet) ermöglicht, anderen Geräten im Netzwerk, üblicherweise Computern, temporäre IP-Adressen zuzuweisen.

DMZ (*Demilitarized Zone*) - Hebt den Firewall-Schutz des Gateways für einen Computer auf, so dass dieser im Internet „sichtbar“ wird.

DNS (*Domain Name Server*) - Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

Domäne - Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

DSL (*Digital Subscriber Line*) - Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

DSSS (*Direct-Sequence Spread-Spectrum*) - Eine bestimmte Art der Funkübertragungstechnologie, die ein redundantes Bit-Muster enthält, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken. Wird für 802.11b-Netzwerke verwendet.

DTIM (*Delivery Traffic Indication Message*) - Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz drahtloser Verbindungen beitragen kann.

Durchsatz - Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

Dynamische IP-Adresse - Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

Ethernet - IEEE-Standardnetzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

Finger - Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

Firewall - Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.

Firmware - 1. Die Programmierung in Netzwerkgeräten, mit der das Gerät gesteuert wird. 2. In den Lesespeicher (ROM) bzw. programmierbaren Lesespeicher (PROM) geladene Programmierung, die von Endbenutzern nicht geändert werden kann.

Fragmentierung - Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über ein Netzwerkmedium, das die ursprüngliche Größe des Pakets nicht unterstützt.

FTP (*File Transfer Protocol*) - Standardprotokoll für das Senden von Dateien zwischen Computern über ein TCP/IP-Netzwerk und das Internet.

Gateway - System zur Verbindung von Netzwerken untereinander.

Halbduplex - Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

Hardware - Als Hardware bezeichnet man die physischen Geräte im Bereich Computer und Telekommunikation sowie andere Informationstechnologiegeräte.

Herunterladen - Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

Hochfahren - Starten des Computers, so dass dieser Befehle ausführt.

HTTP (*HyperText Transport Protocol*) - Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird.

IEEE (*The Institute of Electrical and Electronics Engineers*) - Unabhängiges Institut, das Standards für den Netzwerkbetrieb entwickelt.

Infrastruktur - Die aktuell installierten Computer und Geräte im Netzwerk.

Infrastrukturmodus - Konfiguration, bei der ein Wireless-Netzwerk über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

IP (*Internet Protocol*) - Zum Senden von Daten über das Netzwerk verwendetes Protokoll.

IP-Adresse - Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

IPCONFIG - Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse eines bestimmten Geräts im Netzwerk anzeigt.

IPSec (*Internet Protocol Security*) - VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

ISM-Band - Bei Übertragungen im Wireless-Netzwerkbetrieb verwendetes Funkband.

ISP (*Internet Service Provider*) - Internetdienstanbieter; Anbieter, über den auf das Internet zugegriffen werden kann.

Kabelmodem - Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

Knoten - Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

Laden - Das Übertragen einer Datei über das Netzwerk.

LAN (*Local Area Network*) - Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.

MAC-Adresse (*Media Access Control*) - Die eindeutige Adresse, die ein Hersteller einem jeden Netzwerkbetriebsgerät zuweist.

MBit/s (Megabit pro Sekunde) - Eine Million Bit pro Sekunde. Messeinheit für die Datenübertragung.

Multicasting - Das gleichzeitige Senden von Daten an mehrere Ziele.

NAT (*Network Address Translation*) - Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

Netzwerk - Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam nutzen, speichern und untereinander übertragen können.

NNTP (*Network News Transfer Protocol*) - Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

OFDM (*Orthogonal Frequency Division Multiplexing*) - Eine bestimmte Art der Modulationstechnologie, bei der der Datenstrom in eine Reihe von Datenströmen mit geringerer Geschwindigkeit geteilt wird, die dann parallel übertragen werden. Wird in 802.11a- und 802.11g-Netzwerken sowie beim Netzwerkbetrieb über Stromkabel verwendet.

Paket - Eine Dateneinheit, die über ein Netzwerk gesendet wird.

Passphrase - Wird wie ein Kennwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Verschlüsselungsschlüssel erstellt werden.

Ping (*Packet INternet Groper*) - Internetdienstprogramm, mit dem bestimmt werden kann, ob eine bestimmte IP-Adresse online ist.

POP3 (*Post Office Protocol 3*) - Standardprotokoll, das zum Abrufen von E-Mails verwendet wird, die auf einem Mail-Server gespeichert sind.

Port - 1. Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an dem ein Kabel oder ein Adapter angeschlossen wird. 2. Der virtuelle Anschlusspunkt, über den ein Computer auf eine bestimmte Anwendung auf dem Server zugreift.

PPPoE (*Point to Point Protocol over Ethernet*) - Eine Art Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Kennwort) bietet.

PPTP (*Point-to-Point Tunneling Protocol*) - VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art Breitbandverbindung verwendet.

Präambel - Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

Puffer - Ein Speicherblock, der vorübergehend Daten zur späteren Bearbeitung zurückhält, wenn ein Gerät zum betreffenden Zeitpunkt zu beschäftigt ist, um die Daten zu empfangen.

RJ-45 (*Registered Jack-45*) - Ethernet-Anschluss für bis zu acht Drähte.

Roaming - Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne die Verbindung zu unterbrechen.

Router - Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden, wie beispielsweise das lokale Netzwerk und das Internet.

RTS (*Request To Send*) - Ein Paket, das gesendet wird, wenn ein Computer über Daten zur Übertragung verfügt. Der Computer wartet den Eingang einer CTS-Mitteilung (*Clear To Send*) ab, bevor die Daten gesendet werden.

Server - Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

SMTP (*Simple Mail Transfer Protocol*) - Das standardmäßige E-Mail-Protokoll im Internet.

SNMP (*Simple Network Management Protocol*) - Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

Software - Befehle für den Computer. Ein Satz an Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, bezeichnet man als „Programm“.

SSID (*Service Set IDentifier*) - Der Name Ihres Wireless-Netzwerks.

Standard-Gateway - Ein Gerät, über das der Internetdatenverkehr von Ihrem LAN weitergeleitet wird.

Statische IP-Adresse - Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

Statisches Routing - Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

Streuspektrum - Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

Subnetzmaske - Ein Adressencode, der die Größe des Netzwerks festlegt.

Switch - 1. Gerät, das den zentralen Verbindungspunkt für Computer und andere Geräte in einem Netzwerk darstellt, so dass Daten bei voller Übertragungsgeschwindigkeit gemeinsam genutzt werden können. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen.

TCP/IP (*Transmission Control Protocol/Internet Protocol*) - Ein Netzwerkprotokoll zum Übertragen von Daten, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

Telnet - Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf entfernte Computer.

TFTP (*Trivial File Transfer Protocol*) - Eine Version des TCP/IP-FTP-Protokolls, das UDB verwendet und über keinerlei Verzeichnis- oder Kennwortfunktionalitäten verfügt.

Topologie - Die physische Anordnung eines Netzwerks.

TX-Rate - Übertragungsrate.

UDP (*User Datagram Protocol*) - Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

URL (*Uniform Resource Locator*) - Die Adresse einer sich im Internet befindlichen Datei.

Verschlüsselung - Die Kodierung von Daten, um diese vor einem Zugriff durch nicht autorisierte Dritte zu schützen.

Vollduplex - Die Fähigkeit eines Netzwerkgeräts, Daten gleichzeitig empfangen und übertragen zu können.

VPN (*Virtual Private Network*) - Sicherheitsmaßnahme zum Schutz von Daten im Internet zwischen dem Verlassen eines Netzwerks und dem Eingehen bei einem anderen.

WAN (*Wide Area Network*) - Das Internet.

WEP (*Wired Equivalent Privacy*) - Eine hochgradig sichere Methode zum Verschlüsseln von Daten, die in einem Wireless-Netzwerk übertragen werden.

WINIPCFG - Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse für ein bestimmtes Netzwerkbetriebsgerät anzeigt.

WLAN (*Wireless Local Area Network*) - Eine Reihe von Computern und Geräten, die über Funkverbindungen miteinander kommunizieren.

Anhang G: Spezifikationen

Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), T1.413i2, UR-2 Deutsche Telekom (nur Deutschland)
Ports	Netzstrom, LINE (ADSL), Ethernet (1-4)
Tasten	Reset-Taste, Ein-/Aus-Taste
Kabeltyp	UTP Kat. 5 oder höher
Datenrate	Bis zu 54 MBit/s im Wireless-Betrieb Bis zu 8 MBit/s im ADSL-Downstream-Betrieb Bis zu 800 KBit/s im ADSL-Upstream-Betrieb
Übertragungsleistung	18 dBm
LEDs	Netzstrom, Ethernet (1-4), Wireless-G WLAN, DSL, Internet
Sicherheitsmerkmale	WEP
WEP-Schlüssel	64 Bit, 128 Bit
Abmessungen (B x H x T)	186 mm x 48 mm x 188 mm
Gerätegewicht	0,48 kg
Stromversorgung	Extern, 12 V GS, 1 A
Zertifizierungen	FCC Teil 15B Klasse B, FCC Teil 15C Klasse B, FCC Teil 68, UL 1950, CSA, CE

Betriebstemperatur	0 ºC bis 40 ºC
Lagertemperatur	-20 ºC bis 70 ºC
Luftfeuchtigkeit bei Betrieb	10 % bis 85 %, nicht kondensierend
Luftfeuchtigkeit bei Lagerung	5 % bis 90 %, nicht kondensierend

Anhang H: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Erhöhen Sie den Abstand zwischen der Ausrüstung oder den Geräten.
- Schließen Sie das Gerät an eine andere Buchse als an die des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung
Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte in einem Mindestabstand von 20 cm zwischen dem Heizer und Ihrem Körper installiert und betrieben werden.

KANADISCHE INDUSTRIEBESTIMMUNGEN

Dieses digitale Gerät der Klasse B erfüllt die kanadischen Bestimmungen der Richtlinie ICES-003.
Bei der Verwendung dieses Geräts innerhalb eines Systems, das teilweise oder vollständig im Freien betrieben wird, ist es möglicherweise gemäß kanadischen Bestimmungen erforderlich, eine Genehmigung für das System zu beantragen.

EU-KONFORMITÄTSERKLÄRUNG (EUROPA)

Linksys erklärt, dass das Wireless-G ADSL-Gateway die unten stehenden Spezifikationen erfüllt und den Bestimmungen der europäischen R&TTE-Richtlinie 1999/5/EC nachkommt:

- EN 301 489-1, 301 489-17 EMV-Voraussetzungen für Funkausrüstungen
- EN 609 50 Sicherheit
- EN 300-328-1, EN 300-328-2 Technische Voraussetzungen für Funkausrüstungen

Warnung: Dieses Gerät ist zur Verwendung in allen EU- und EFTA-Mitgliedsstaaten bestimmt. Die Verwendung im Freien ist u. U. auf bestimmte Frequenzen beschränkt bzw. erfordert eine Betriebslizenz. Informationen zur Verfahrensweise erhalten Sie von der örtlichen Behörde.

Hinweis: Kombinationen von Leistungspegeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW (EIRP; *Effective Isotropic Radiated Power*) führen, erfüllen nicht die Bestimmungen der oben genannten Richtlinien und sind deshalb nicht für die Verwendung innerhalb der EU und jenen Ländern zulässig, die die europäische Richtlinie R&TTE 1999/5/EC übernommen haben.

Weitere Informationen zu rechtlich zulässigen Kombinationen von Leistungspegeln und Antennen erhalten Sie von der Abteilung für Unternehmensvorschriften von Linksys.

- Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
- Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.
- Belgique:

  Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.
- France:

  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le department. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

FCC TEIL 68 ERKLÄRUNG

Dieses Gerät entspricht Teil 68 der FCC-Bestimmungen. Am Gerät befindet sich ein Etikett, das u. a. die FCC-Registrierungsnummer und die Rufäquivalenzzahl (*Ringer Equivalence Number*; REN) des Geräts aufweist. Falls erforderlich, müssen Sie der Telefongesellschaft diese Angaben mitteilen.

Dieses Gerät verwendet die folgende USOC-Buchse: RJ-11.

Im Lieferumfang dieses Geräts sind ein FCC-kompatibles Telefonkabel und ein Modularstecker enthalten. Dieses Gerät ist zum Anschluss an das Telefon- oder Unternehmensnetz mithilfe eines kompatiblen Modularsteckers bestimmt, der FCC Teil 68 entspricht. Die Verbindung zum Telefonnetz sollte über die Standardmodularbuchse für Telefonverbindungen hergestellt werden.

Mit der REN kann die Anzahl der Geräte ermittelt werden, die an die Telefonleitung angeschlossen werden können. All diese Geräte können einen Klingelton abgeben, wenn Ihre Telefonnummer gewählt wird. In den meisten (nicht allen) Fällen sollte die Gesamtzahl der RENs nicht 5 überschreiten. Um die Anzahl der Geräte, die gemäß der Gesamtzahl der RENs an die Leitung angeschlossen werden können, zu überprüfen, wenden Sie sich an die Telefongesellschaft; diese informiert sie über die maximale Anzahl an RENs für den Anrufbereich.

Wenn durch dieses Gerät Schäden am Telefonnetz verursacht werden, kann die Telefongesellschaft Ihren Dienst vorübergehend einstellen. Wenn keine Vorankündigungen möglich sind, wird die Telefongesellschaft den Kunden so früh wie möglich benachrichtigen. Sie werden außerdem über Ihr Recht in Kenntnis gesetzt, eine Beschwerde bei der FCC einzureichen, falls Sie dies als notwendig erachten.

Die Telefongesellschaft nimmt u. U. Änderungen an ihrem System, ihrer Ausrüstung, ihrer Betriebs- oder Vorgehensweise vor, die den Betrieb des Geräts beeinträchtigen können. In diesem Fall kündigt die Telefongesellschaft dies im Voraus an, so dass Sie die für einen durchgehenden Betrieb nötigen Änderungen vornehmen können.

Sollte dieses Gerät nicht einwandfrei funktionieren, trennen Sie es von der Telefonleitung. Versuchen Sie, ein anderes FCC-kompatibles Gerät in derselben Telefonbuchse zu verwenden. Falls das Problem weiterhin besteht, wenden Sie sich an den Kundendienst der Telefongesellschaft. Falls das Problem behoben ist und somit im Gerät vorzuliegen scheint, trennen Sie das Gerät von der Telefonleitung, und verwenden Sie es erst nach entsprechender Reparatur wieder. Bitte beachten Sie, dass Sie von der Telefongesellschaft dazu aufgefordert werden können, das Gerät vom Telefonnetz zu trennen, bis das Problem behoben ist oder bis Sie sichergestellt haben, dass keine Funktionsstörung im Gerät vorliegt. Für eine optimale Leistung des Geräts sind Zubehör und Kabel vom Hersteller zu verwenden.

Vom Kunden sind keine Reparaturarbeiten vorzunehmen. Wenn bei Verwenden dieses Geräts Probleme auftreten, erhalten Sie bei einem autorisierten Kundendienstanbieter Informationen zu Reparatur- und Garantieleistungen. Wenn das Problem Schäden am Telefonnetz hervorruft, können Sie von der Telefongesellschaft dazu aufgefordert werden, das Gerät vom Netz zu trennen, bis das Problem behoben ist. Dieses Gerät kann nicht mit von der Telefongesellschaft bereitgestellten Münzfernsprechern verwendet werden. Die Verbindung zu einem Gemeinschaftsanschluss-Dienst unterliegt der staatlichen Gebührenordnung.

SICHERHEITSHINWEISE

- Warnung: Verwenden Sie zur Reduzierung der Brandgefahr ein Telefonkabel der AWG-Klasse Nr. 26 oder größer.
- Verwenden Sie dieses Gerät nicht in der Umgebung von Wasser, wie z. B. in einem feuchten Keller oder in der Nähe eines Schwimmbeckens.
- Vermeiden Sie die Verwendung dieses Produkts (außer der kabellosen Variante) während eines Gewitters. Es besteht das (geringe) Risiko eines elektrischen Schlags durch Blitzschlag.

Anhang I: Garantieinformationen

Eingeschränkte Gewährleistung

Linksys sichert Ihnen für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist“) zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigener Wahl das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Kundendienst von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN KUNDENDIENST WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre eigene Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanada sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen bei Ihnen keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGSTHEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss bzw. keine Beschränkungen von zufälligen oder mittelbaren Schäden; die oben genannte Beschränkung oder der oben genannte Ausschluss finden daher unter Umständen bei Ihnen keine Anwendung.

Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA.

Anhang J: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits etablierte Produkte finden Sie online unter:
http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

In Europa	E-Mail-Adresse
Belgien	support.be@linksys.com
Dänemark	support.dk@linksys.com
Deutschland	support.de@linksys.com
Frankreich	support.fr@linksys.com
Großbritannien & Irland	support.uk@linksys.com
Italien	support.it@linksys.com
Niederlande	support.nl@linksys.com
Norwegen	support.no@linksys.com
Österreich	support.at@linksys.com
Portugal	support.pt@linksys.com
Schweden	support.se@linksys.com
Schweiz	support.ch@linksys.com
Spanien	support.es@linksys.com

Außerhalb von Europa	E-Mail-Adresse
Lateinamerika	support.la@linksys.com
USA und Kanada	support@linksys.com